

COVID-19 FRAUD AND SCAM

**SCAM
ALERT!**



COVID-19 community forum: Fraud, waste and abuse

July 9, 2020

Agenda

- What are COVID-19 fraud schemes?
- What do COVID-19 schemes sound like?
 - Phone calls – robocalls, impersonators
- What do COVID-19 schemes look like?
 - Online and social media ads, emails with links, attachments
- You can protect yourself against scams and fraud
- Report scams and fraud
- Resources to help you stay safe

What are COVID-19 fraud schemes?

Aggressive scams playing on public fears around COVID-19 that use tricks or threats to:

- Steal your money
- Get access to your personal information, like your Medicare or Medicaid number, your date of birth or address
- Secretly install malicious software on your computer so they can get your personal information, like passwords, bank account numbers or social security number

What do COVID-19 schemes sound like?

1. Home delivery of home supplies



2. Free diabetes monitor and COVID-19 test



3. Free coronavirus test kit delivered immediately



What do COVID-19 schemes sound like?



What do COVID-19 schemes look like?

IRS COVID-19 News:

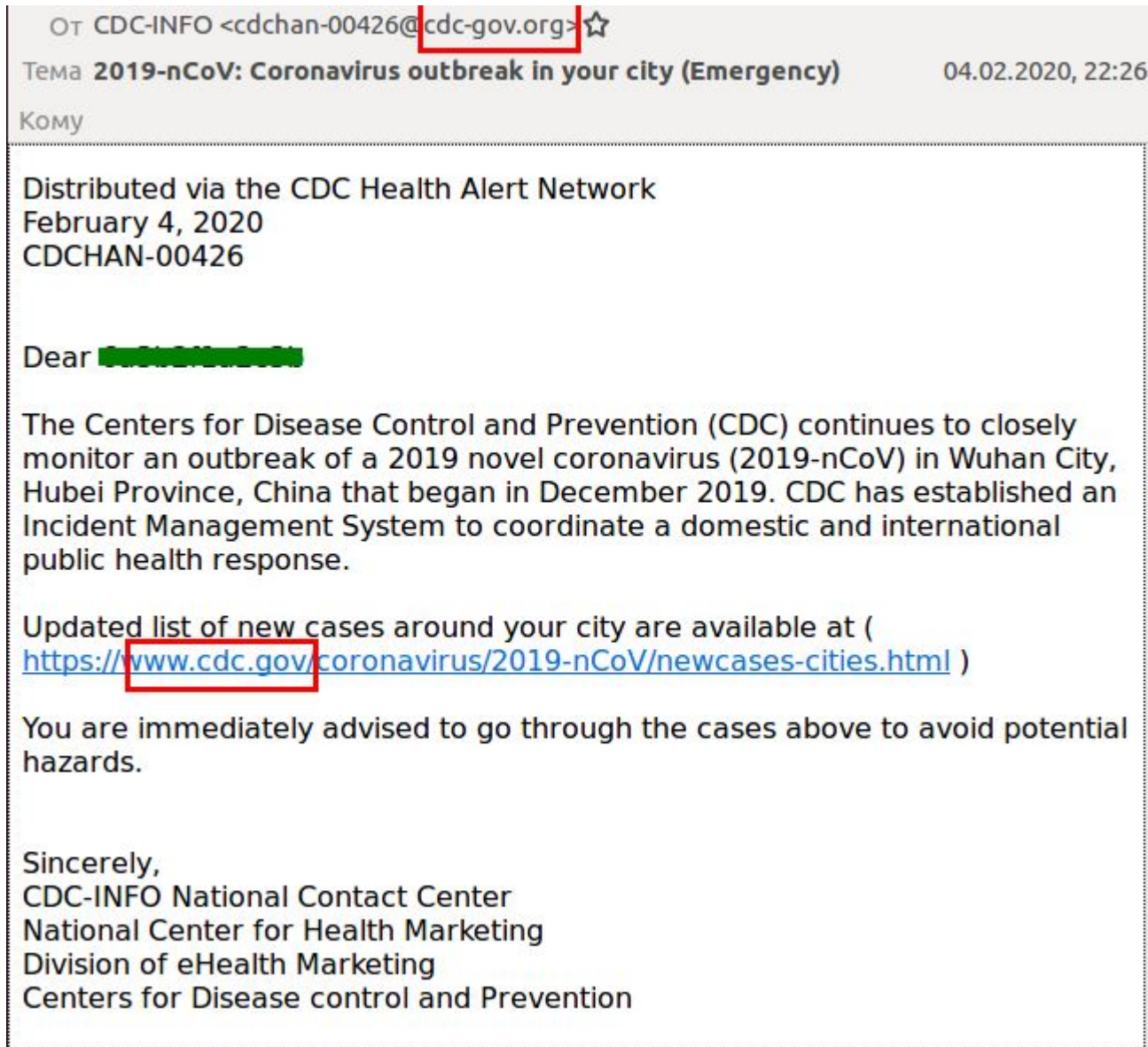
Click [xxx.xxx/IRS-COVID-19](#) to register/update your information in order to receive the economic impact payment regardless of your status.

What do COVID-19 schemes look like?

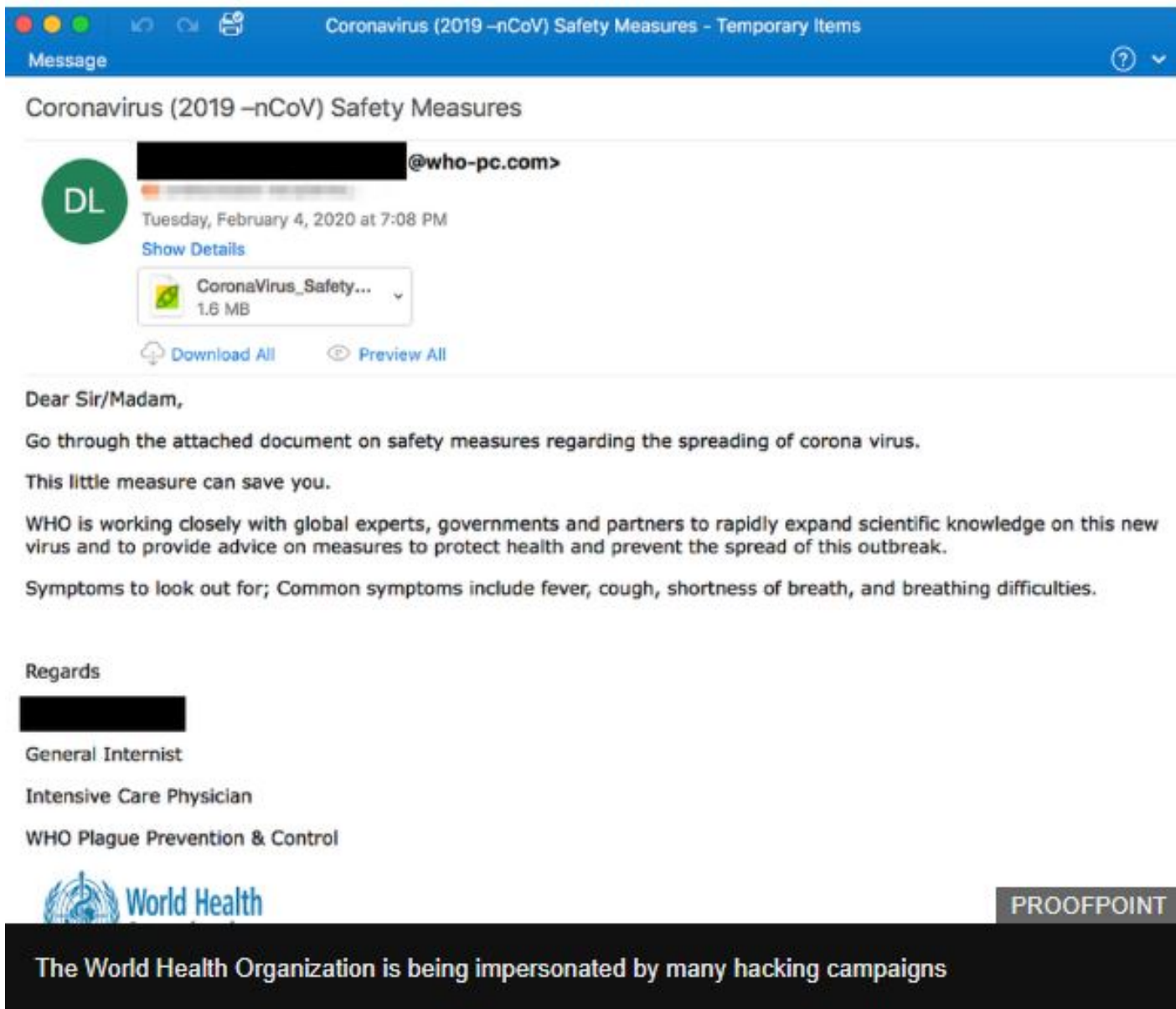
YiLo * COVID-19 cautions cont.
Coronav Immunization
Stabilizer Tincture Now
Available WSL, 10% OFF Online
Leafly Orders Continues
<http://yeatic.com/reMGBDR>



What do COVID-19 schemes look like?



What do COVID-19 schemes look like?



The image shows a screenshot of an email interface. The window title is "Coronavirus (2019 -nCoV) Safety Measures - Temporary Items". The email header shows the subject "Coronavirus (2019 -nCoV) Safety Measures" and the sender as a redacted name with the email address "@who-pc.com". The email is dated "Tuesday, February 4, 2020 at 7:08 PM" and includes a "Show Details" link. An attachment is visible: "CoronaVirus_Safety..." (1.6 MB). Below the attachment are "Download All" and "Preview All" options. The email body contains the following text:

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[Redacted Name]

General Internist
Intensive Care Physician
WHO Plague Prevention & Control

The email footer features the World Health Organization logo and the text "World Health". A grey box on the right contains the word "PROOFPOINT". A black banner at the bottom of the email contains the text: "The World Health Organization is being impersonated by many hacking campaigns".

What do COVID-19 schemes look like?

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission



CDC INFO <CDC-Covid19@cdc.gov>

To: [REDACTED]

Reply

Reply All

Forward

Wed 2/26/2020 12:00

As you know, the Department of Health and Human Services has declared the Coronavirus (COVID-19) a public health emergency.

At this time, three new cases have been confirmed around your location today. The risk to the Public in your city and throughout the World is very HIGH.

The World Health Organization has named the new coronavirus, Covid-19, and the Centers for Disease Control and Prevention has established precautions.

* The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chances for Exposures.

* A high-risk person is currently being monitored around your city center.

For additional information about high-risk places around

<https://healing-yui223.com/cd.php?>

Click or tap to follow link.

<https://www.cdc.gov/COVID-19/newcases/feb26/your-city.html>

COFENSE

Hackers are using fear-mongering tactics to encourage clicks and downloads

What do COVID-19 schemes look like?

Schemes sometimes start online but can turn into you visiting a medical office.

Let's look at one example.

A case study: Harmony Medical Care



TAKE CONTROL OF YOUR HEALTH DURING
THESE UNCERTAIN TIMES.

(This is not a video. It is only an image.)

Proprietary and Confidential

A case study

On May 25, 2020, the U.S. Attorney's Office for the District of Arizona filed a criminal complaint charging Jeremiah Faber, the CEO of Harmony Medical Care, with health care fraud and money laundering.

[The complaint alleges](#) that Faber used Harmony's Facebook and other social media sources to offer free COVID-19 testing in order to induce patients to also complete Harmony's Comprehensive Whole-Body Assessment.

The complaint documents the case of one patient who visited Harmony for the free COVID-19 test. This patient was then given additional services that were medically unnecessary. The complaint further alleges that Harmony subsequently submitted false claims to Mercy Care by billing for these medically unnecessary services under the names of physicians who had no involvement with the patient's testing.

Ways to protect yourself against becoming a victim of fraud

KEEP CALM and Avoid Coronavirus Scams

Here are **5 things** you can do to avoid a Coronavirus scam:



Ignore offers for vaccinations and home test kits.

Scammers are selling products to treat or prevent COVID-19 without proof that they work.



Hang up on robocalls.

Scammers use illegal sales call to get your money and your personal information.



Watch out for phishing emails and text messages.

Don't click on links in emails or texts you didn't expect.



Research before you donate.

Don't let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.



Stay in the know.

Go to ftc.gov/coronavirus/scams for the latest information on scams. Sign up to get FTC's alerts at ftc.gov/subscribe.

You can protect yourselves



You can protect yourselves



Avoid Coronavirus Scams
FTC Tip # 2
**Ignore offers for
vaccinations and
home test kits**

ftc.gov/coronavirus
bbb.org/coronavirus

You can protect yourselves



Avoid Coronavirus Scams

FTC Tip # 8

**Do your homework
when it comes to donations**

If someone wants donations in cash,
by gift card, or by wiring money,
don't do it.

Resources to keep you alert against COVID-19 schemes

Fraudsters and scammers are constantly changing their approach and developing new ways to use COVID-19 to trick and threaten companies and individuals out of sensitive information or money.

Get the latest alerts about COVID-19-related schemes and fraudulent activity:

- [AZ Attorney General's COVID-19 Consumer Protection](#)
- [FBI Internet Crime Complaint Center \(IC3\): Fraud Alerts](#)
- [Federal Trade Commission Coronavirus Consumer Advice](#)

How to report COVID-19 fraud and schemes

For individuals with AHCCCS, also known as Medicaid:

- AHCCCS members must report fraud, waste, and abuse to the AHCCCS Office of Inspector General on their website at <https://www.azahcccs.gov/Fraud/ReportFraud/>.
- You can send an email to AHCCCSFraud@azahcccs.gov.
- You can also call the Fraud Hotline at 602-417-4193 or 1-888-487-6686.

How to report COVID-19 fraud and schemes

For individuals with Medicare or Medicare *and* Medicaid coverage, such as Mercy Care Advantage:

If you believe you have been a target of a coronavirus-related scam, or know someone else who has been, you should report the fraud.

You can report it to Mercy Care or Medicare:

- Medicare fraud: **1-800-633-4227**
- Mercy Care Fraud Hotline at **1-800-810-6544**.

Questions?

Thank You

