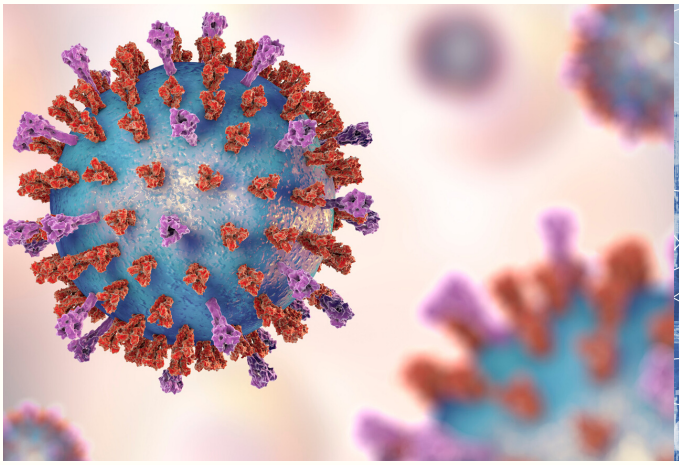
MARCH 24, 2020 VOL. 1

Edelson PRIVACY NEWSLETTER

As Part of Edelson PC's COVID-19 Task Force



A Message to the Community

As COVID-19 continues to have an impact on the world, we understand this is a challenging time for everyone. In order to practice social isolation, many people are struggling to quickly adapt to new technologies for work as well as to remotely keep in contact with friends and family.

Unfortunately, this increased online presence has presented even more opportunities for malicious individuals to target people with new online threats and scams.

The inaugural issue of this newsletter will provide tips for avoiding these new schemes as well as general tips to stay safe online.

Learn more about our efforts to help consumers and the community during the COVID-19 pandemic at: https://edelson.com/covid-19-task-force

Together, we'll stay strong.

Edelson

IN THIS ISSUE

Protecting Yourself Against COVID-19 Online Threats and Scams

Our firm staffs in-house technology experts that investigate various security and privacy abuses to protect consumers. These same experts have provided tips on how to protect yourself against threats specifically related to COVID-19.

1. Social Engineering

Social engineering is the art of manipulating people into giving up confidential information or taking an action. The main types of social engineering generally occur either via email (Phishing) or voice on the phone (Vishing).

Some phishing schemes are broad and wide in order to affect as many people as possible. Narrow and targeted phishing emails towards specific people or groups are called spear phishing. The main goal of phishing is to convince a person to either:

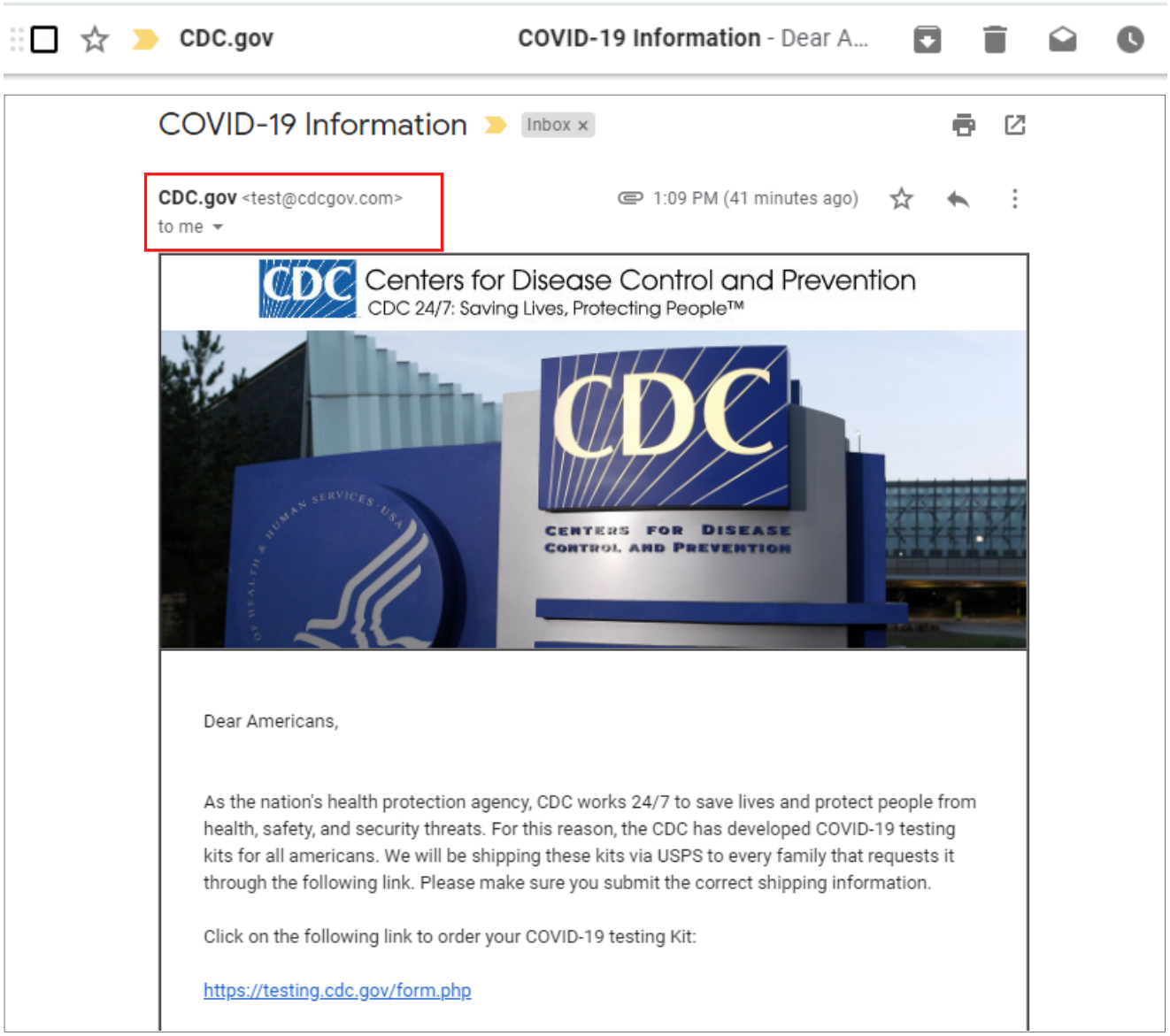
- Reply to an email and provide confidential information
- Click on a link that leads to a malicious website
- Open a malicious attachment

Verify the Sender Before Replying

The below email provides a good example of a potential COVID-19 phishing scheme purportedly from "CDC.gov." Here, the attacker faked the sender name as CDC.gov and put a sender email address of cdcgov.com (which the attacker will receive the replies to and is similar to the real cdc.gov domain).

The attacker could have faked the sender email address as the legitimate cdc.gov domain as well, but then the attacker would not receive the replies. In that scenario, the attacker would rely more on the victim clicking a malicious link or opening an attachment.

Therefore, err on the side of caution, and avoid replying to any email that asks for sensitive information unless you have verified the request was real via the organization's phone number listed on their website. Avoid using a phone number listed in an email to call for verification.

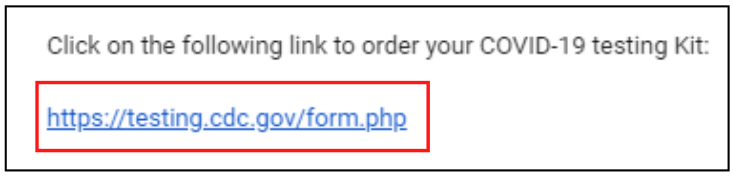


Don't Click on Links Blindly

Be very careful when receiving a suspicious email that wants you to click on a link. Attackers often embed malicious links in emails that either:

- Lead to a fake page to capture your email and password such as Gmail, your bank, etc.
- Lead to a malicious server that will try to infect your device with malware.

The example email wants you to click on the link to order a COVID-19 testing kit. At first glance, the link looks legitimate and appears to lead to cdc.gov. However, clicking on this link would actually lead to cdcgov.com (which is controlled by the attacker and is not a legitimate CDC site).

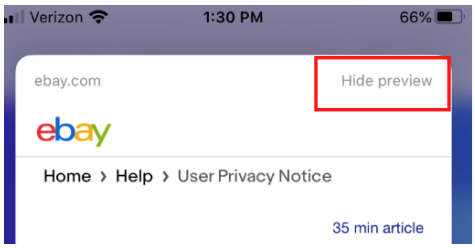


Luckily, most email software allows you to see the actual destination of a link by hovering over it with your mouse. If you don't see the destination when hovering, another tip is to copy and paste the link into a notes app.

You can also verify links in emails on your phone as well. In Android, simply long click on the link to see the actual destination. For an iPhone, you can also long click, but should turn off the preview mode first as described below.

iPhone Steps to Turn Off Preview Mode

1. Click on a known good link in an email and select "Hide preview" to turn preview mode off.

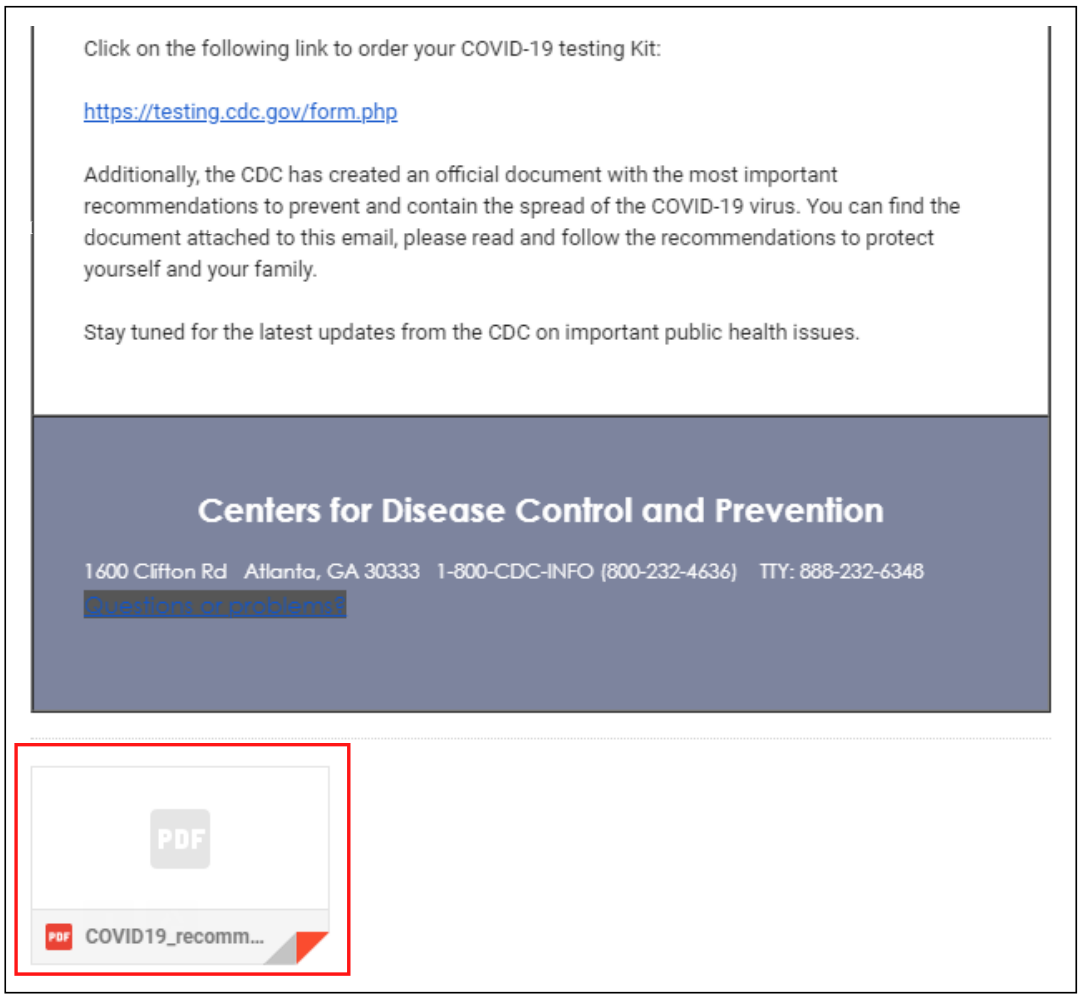


2. Now, when you see a link in an email, simply long hold on the link to see the true destination. Simply click somewhere else on the screen to avoid visiting the site if it appears to not match the legitimate website's domain.

Illegitimate Domain

Avoid Opening Attachments Blindly

Be especially careful not to open any attachments in an email unless you are absolutely sure who the sender is. Many malicious attachments are filled with malware that oftentimes will disable your antivirus software in order to download additional malware such as a keylogger. A keylogger can be used to capture your logon credentials to various websites which will then be sent to the attacker. Our example phishing email contains the below malicious PDF attachment:



Common COVID-19 Phishing Schemes

Some COVID-19 related phishing schemes to avoid are:

- Emails claiming to be from the CDC, the WHO, or other health agencies
- Any email or online offer for a COVID-19 vaccination or other "cure"
- An email claiming to be from your employer or school relating to COVID-19

The following are examples of COVID-19 phishing attempts as reported by the U.S. Department of Health and Human Services:

"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before **[[current_date_1]]**.

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

Singapore Specialist : Corona Virus Safety Measures

DT [redacted]
Tuesday, 28 January 2020 at 03:51
[redacted]
Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Be Suspicious of Phone Calls or Visits Related to COVID-19

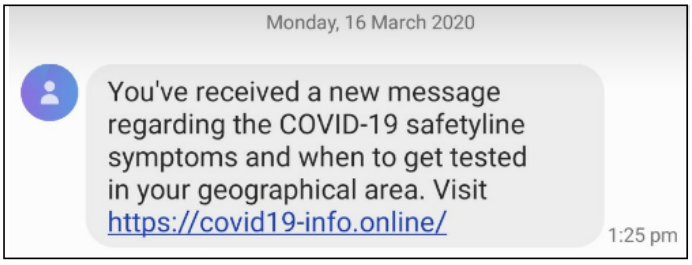
Common voice based social engineering campaigns (Vishing) generally begin with a pre-recorded message that prompts the victim to call a toll free number. These calls are generally answered by an interactive voice response (IVR) system or a live operator to attempt to induce the victim to provide sensitive information that can later be used for identity theft. Other Vishing methods include via a text message or a live person calling. Some people have also reported scammers showing up at their home with fake test kits for sale.

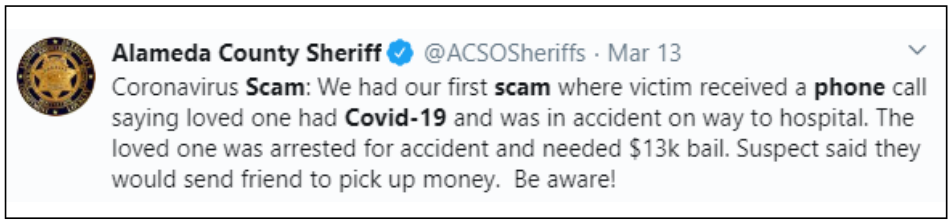
Common phone or visit based schemes include:

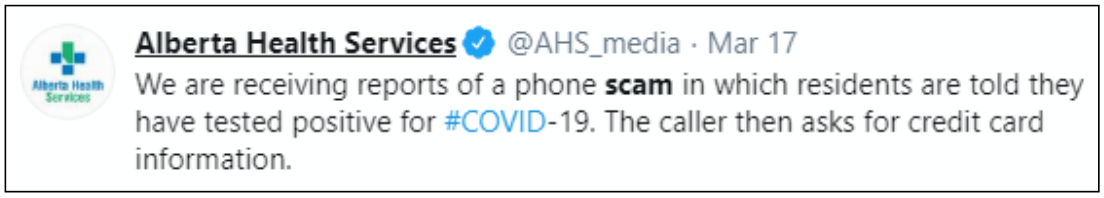
- The IRS or Social Security Administration requesting money or information
- Anyone that asks for a gift card
- A local or federal law enforcement agency claiming you will be arrested if you don't pay a fine
- You have been selected for a cruise, prize, etc.
- A pretend call from your bank, work, a utility company, or a school

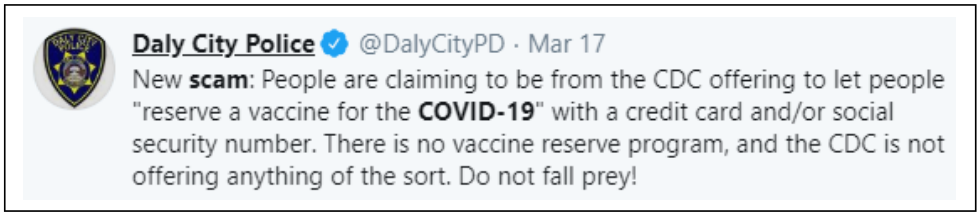
---

The following are examples of phone based scams related to COVID-19:





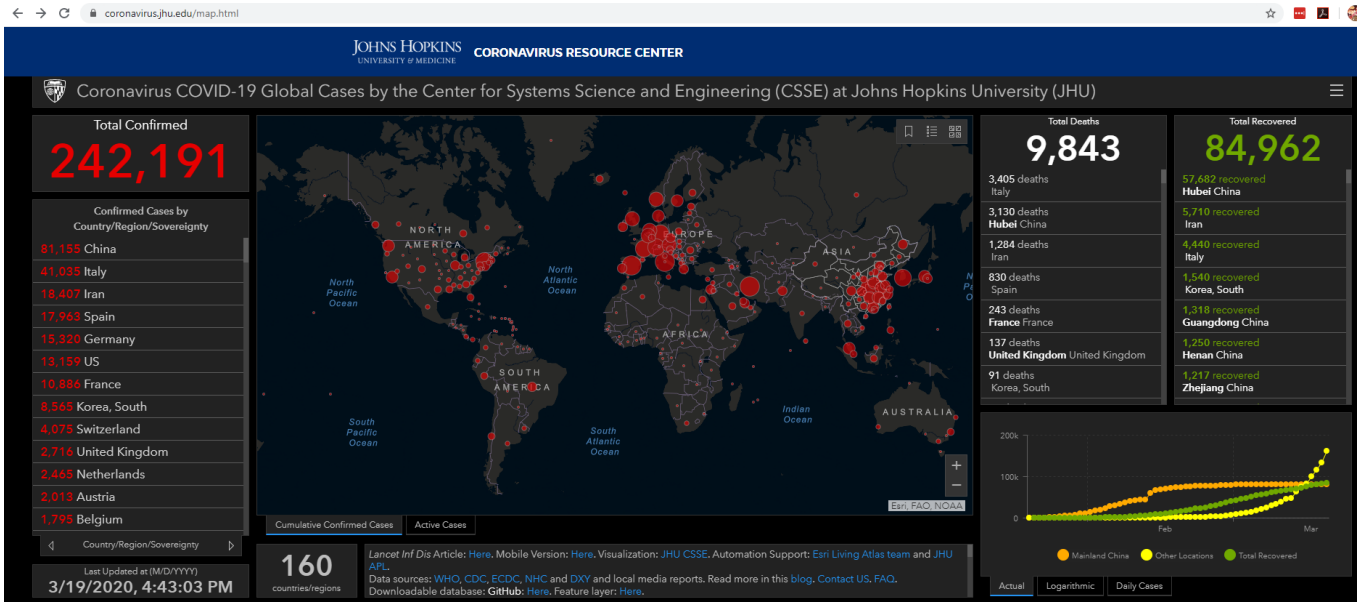




2. Fake COVID-19 Trackers

Johns Hopkins University designed a popular COVID-19 tracker which details the total infections, deaths, and recoveries in each country. Attackers have recently started creating several fake variants of the Johns Hopkins tracker with the goal of installing spyware on the victim's computer or mobile device.

In order to access the legitimate tracker, you can visit: https://coronavirus.jhu.edu/map.html.



Avoid the following:

- Interacting with any emails that claim to have a link or attachment to the tracker
- Installing any mobile apps that claim to be a COVID-19 tracker
- Visiting any suspicious website that claims to be a COVID-19 tracker. A few other legitimate trackers include:
  - https://covidtracking.com
  - https://ncov2019.live

3. Disinformation Campaigns

Several media outlets have reported that a European Union database has recorded roughly 80 cases of disinformation regarding COVID-19 so far. The campaigns are designed to generate panic and cause distrust by falsely claiming that the Coronavirus is a biological weapon created by the West.

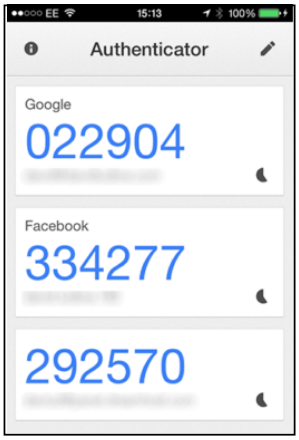
The U.S. Government has also alleged foreign disinformation campaigns are attempting to spread fear be making false claims that U.S. service members created and are spreading the virus as well as stoking fears of a nationwide military quarantine.

Please keep in mind that it is very easy for attackers to create fake social media accounts in order to spread false information. Social media companies have processes in place to try to detect these campaigns, but many slip through the cracks. Avoid blindly trusting what is posted online and instead refer to the websites of world, national, state, and local health and government organizations to receive accurate updates regarding COVID-19.

4. Other General Security Tips

The following are other general tips to ensure you are staying safe online, not only during COVID-19, but in general as well.

- **Use 2 factor authentication for your bank, email, and other accounts that contain sensitive or financial information**



- **Use a password manager to set individual strong and unique passwords for each site that you use***

  ***You then only have to remember your single master password.**

- Change the default passwords on your router, webcams, and any other IoT devices in your home

- Avoid using sites that are not encrypted (HTTP) and use HTTPS sites instead or a VPN

- Be aware that malware is often contained in software downloads, browser extensions, toolbars, and mobile apps from non-reputable sources

- Lock your device when not in use, and use full disk encryption on devices that contain sensitive information*

Turn any computer with full disk encryption completely off before traveling or leaving it unattended for an extended period of time. Otherwise, attackers can potentially grab the decryption key from the RAM of a computer that is running or in sleep mode in order to access your files.