# COVID-19 (Coronavirus) Scams and Tips to Help Prevent Exploitation


## Summary:

The COVID-19 (Coronavirus) pandemic is creating opportunities for scammers to take advantage of people. There are a variety of techniques that bad actors can use to exploit uncertainty caused by the pandemic, from fake online offers to email phishing schemes. These techniques can be used to steal identities, financial details, or otherwise exploit personal information for fraudulent purposes. Below are some of examples of attempts by scammers and hackers to manipulate people who may be looking for help or looking to provide help to those impacted by COVID-19, along with privacy and cyber security related tips to identify and prevent such scams.


**Please Note**: The content contained in this document may be used to assist with the protection of your personal information (e.g., your identify, credit card details, etc.), while conducting the personal business of you and your family. However, no tips or recommendations below or elsewhere will provide complete protection from all scams or attempts to collect and/or exploit personal and sensitive information, and the County of Santa Clara shall not be held responsible or liable for the information provided in this document. Additionally, this resource includes several links to external sources of information, which may be useful in preventing, managing, and recovering from such scams. Please refer to the County's Links Policy as necessary, available here.

## Potential COVID-19 Scams:

- Sale of Fake Products
  - Buy COVID-19 test kits online
  - Sellers who claim to have medical, health, and cleaning supplies, but never deliver
  - COVID-19 emails or texts that sound too good to be true: Free iPhone
- Requests for Donations to Fake Charities
  - Buy gift cards to help small shop owners
  - Provide donations to assist elderly and other vulnerable people in need of food and assistance
- Phishing Attacks and Social Engineering through Email, Text, and Phone
  - COVID-19 stimulus check scams
  - Driving recipients to click COVID-19 related links to fake charities
  - Urgent action demanded and requesting personal information
  - Ransom attacks embedded in emails
  - Installing malware using COVID-19 Interactive Maps accessed through phishing
- Imposters Posing as Reputable Sources and Misinformation
  - Claims to be World Health Organization (WHO)
  - Cyber-Attack on federal government Health & Human Services (HHS) linked to COVID-19 misinformation efforts
- *Additional Actions to Take and Tips to Consider*
- *How to Protect Yourself Against Scams and Recourse for Victims*
- *COVID-19 Scams Resources*

## Sale of Fake Products

### Buy COVID-19 Test Kit Online

Scammers are contacting consumers via phone and email to get them to verify personal and financial information to purchase fake COVID-19 testing kits. (*Coronavirus fraudsters prey on fear and confusion with fake products, email scams, CNBC*)

- *What you can do:* If you do not recognize the phone number or email of an organization, do not respond or click on any embedded links. Go to reputable sources for information, including the Centers for Disease Control and Prevention (CDC), California Department of Public Health, Santa Clara County Public Health Department, and World Health Organization.

### Sellers Who Claim to Have Medical, Health, and Cleaning Supplies, but Never Deliver

Online sellers claim they have in-demand products, like cleaning, household, and health and medical supplies. You place an order, but you never get your shipment.

- *What you can do:* To avoid this, try searching online for the person or company's name, phone number and email address, plus words like "review," "complaint," or "scam." If everything checks out, consider paying by credit card and keeping a record of your transaction. This will help to refute a charge, if necessary, should you fail to receive a shipment. *(FTC: Coronavirus scams, Part 2)*

### COVID-19 Emails or Texts that Sound too Good to be True

Scammers are sending text messages promising free products, such as iPhones, to people who must spend time at home due to COVID-19. To obtain the product, the recipient is directed to click a link which could lead to downloading malware or other negative outcomes. (*Covid-19 Scams Are Everywhere Right Now. Here's How to Protect Yourself, Time)*

- *What you can do:* If you do not recognize the phone number, email address, text source, or organization; do not respond or click on any embedded links. Go to reputable sources such as the Federal Trade Commission (FTC) for more information and guidance.

## Requests for Donations to Fake Charities

### Buy Gift Cards to Help Shops Closed Because of COVID-19

Consumers are getting lured to fake websites asking for their name and credit card information to purchase online gift cards to help shopkeepers and others impacted by COVID-19. (Fake tests, fantasy cures and false government aid checks: Chicago authorities warn scammers are ramping up as coronavirus spreads, Chicago Tribune)

- *What you can do:* Check out the seller by searching online for the person or company's name, phone number, and email address, plus words like "reviews," "ratings," "complaints," and "scams." If everything checks out, pay by credit card and keep a record of your

transaction. This will help to refute a charge, if necessary, should you fail to receive a shipment. *(FTC: Coronavirus scams, Part 2)*

**Provide Donations to Assist Elderly and Other Vulnerable People in Need of Food and Assistance**

There are several fraud schemes seeking to exploit the COVID-19 public health emergency by targeting vulnerable populations by soliciting donations under the pretense of helping individuals, groups, and those in affected areas. Sometimes it can be difficult to tell the difference between legitimate sites and fraudulent ones. *(U.S. Attorney Shares Tips for Avoiding COVID-19 Scams Targeting Vulnerable Populations, United States Department of Justice)*

- *What you can do:* The top three recommendations given by the Department of Justice U.S. Attorney's Office are:
    - Independently verify the identity of any company, charity, or individual that makes contact regarding COVID-19.
    - Check the websites and email addresses offering information, products, or services related to COVID-19. Be wary of unsolicited emails offering information, supplies, treatment for COVID-19 or requesting your personal information for medical purposes.
    - Legitimate health authorities will not contact the general public this way. *For more of their tips click here.*

## Phishing Attacks and Social Engineering Through Email, Text, and Phone Calls

**COVID-19 Stimulus Check Scams**

Someone calls, texts, or emails claiming that you need to provide personal information to verify your address and direct deposit details to receive the $1,200 stimulus payment from the IRS. (Coronavirus stimulus check scams, USA Today)

- *What you can do:* If you do not recognize the phone number or organization, do not respond or click on any embedded links. Go to reputable sources for information such as the Internal Revenue Service webpage for Coronavirus Tax Relief and the U.S. Treasury webpage on Coronavirus: Resources, Updates, and What You Should Know.

**Driving Recipients to Click COVID-19-related Links to Fake Charities**

Digital fraudsters are sending phishing emails asking recipients to click on embedded links for a variety of reasons (e.g., to show their support for the fight against COVID-19, to donate money, to sign up to receive services if in need, to volunteer to provide services if healthy). *(FTC: Coronavirus scams, Part 2)*

- *What you can do*: Do as much research as possible before donating. Money lost to bogus charities not only means that the giver loses out, but it also means fewer donations go to help those who actually need it. When you give, pay safely by credit card, never by gift card

or wire transfer. Review the FTC's resource on safe giving to charity to avoid fraud at: FTC, Avoid Charity Scams.

**Urgent Action Demanded**

A common tactic with phishing emails is to include "Urgent or immediate action" in the subject line of an email such as this one: "*URGENT: COVID-19 ventilators and patient test delivery blocked. Please accept order here to continue with shipment.*" *(*Phishing in the Time of Coronavirus, Electronic Frontier Foundation*)*

- *What you can do*: If a message's language seems urgent, as though it's attempting to pressure you into giving up your information to avert some sort of data disaster or negative outcome, it could very well be fake. Bad actors know that instilling a sense of urgency can catch people off-guard, create a sense of insecurity, and otherwise serve as a strategy to get people to let common sense take a backseat. If you receive a suspicious email from a particular company or even a friend or your employer, contact them separately via phone or other means to verify the message before replying or otherwise acting on it. *(COVID-19 Scams Are Everywhere Right Now. Here's How to Protect Yourself, Time)*

**Ransom Attack Embedded in COVID-19 Emails**

Consumers are lured into downloading an app, for instance, to receive COVID-19 updates or to track infection trends. Then the appl encrypts and locks the user's mobile device demanding funds, such as Bitcoin, in ransom.

- *What you can do*: The International Institute of Cyber Security (IICS) recommends that users do not install apps from unknown or untested sources, as this is one of the main attack vectors against mobile devices. In addition, for users concerned about the COVID-19 outbreak and its current status, it is always best to expect official updates from health and cyber authorities and their web sites. (COVID-19 Exploited by Malicious Cyber Actors, Joint alert from United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC))

**Installing Malware Using COVID-19 Interactive Maps Accessed through Phishing**

Many organizations such as Johns Hopkins University are using maps to visualize the spread of COVID-19. Scammers are taking advantage of this by creating fake maps that require users to download software, which in turn installs malware (malicious software) on individuals' devices, oftentimes without your knowledge. *(Johns Hopkins University statement on malware disguised as Covid-19 map)*

- *What you can do*: Most legitimate sources will not require the average user to download software in order to view a COVID-19-related map. Other reputable sources are available that can offer you such data, locally and nationally. Remember, always be cautious when clicking on links or downloading software.

## Imposters Posing as Reputable Sources and Misinformation

### Claims to be the World Health Organization (WHO) or Other Institutions

Scammers can disguise communications to make them look as if they are coming from the World Health Organization, Centers for Disease Control and Prevention or other institutions providing information about COVID-19. (Coronavirus Scams: Watch Out for These Efforts to Exploit the Pandemic, Forbes)

- *What to do:* Look carefully at email domains to make sure they match the real organization. Scammers often create domains that contain a slight variation in the organization's correct website domain.


*FTC: Coronavirus scams, Part2*

### Cyber-Attack on Federal Government Health & Human Services (HHS) Linked to Misinformation about COVID-19

In mid-March 2020, the federal government department of HHS suffered a cyber-attack on its network, as well as a misinformation campaign designed to undermine the response to the COVID-19 pandemic. (Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak, Bloomberg)

- *What you can do:* The internet and social media create unique opportunities for spreading misinformation and disinformation. Here are several questions you can ask when trying to distinguish between good information and misleading or false information:
    - Is this the original account, article, or piece of content?
    - Who is sharing or creating it (e.g., ,Are they biased or objective?)?
    - Are they a trusted source?
    - When was it created?
    - What about the account sharing this material or links? When was it created? Is this source sharing information at all times of the day and night? Could it be a bot or other untrusted source?
    - Why is it being shared?

    (5 ways to spot disinformation on your social media feeds, ABC News)

## Additional Actions to Take and Tips to Consider

**Actions to Take:**

The main action to take against phishing scams is to exercise caution before clicking links or attachments that you receive by email, text, or other source. No matter how urgent the communication might sound, it is important to stop and think about the context of the communication and whether there are any clues that might indicate it is not legitimate.

Clues that can help reveal a scam:

- Unknown sources, charities, government sites, or other organizations, especially when combined with a request for urgent action.
- Web sites for organizations with consistent negative reviews relating to privacy protection or track record of service (or phone calls from such organizations) asking you to provide personal information and financial details.
- Obvious grammatical errors in emails from organizations.
- Generic greetings, such has “Hello Sir/Ma’am,” especially from unsolicited sources or entities that you don’t normally correspond with either personally or professionally.
- Hovering the mouse pointer over an embedded link reveals a pop-up link that seems to have no relationship to the sender.

You can also get someone else’s opinion. Ask a coworker or other trusted source: Were we expecting an email from this sender? Or ask a friend: Does this email look strange to you?

A good practice is to use a different medium to verify whether a communication is genuine (For example, if you receive a strange email claiming to be from your friend, try calling your friend over the phone to double-check that it’s from them.). If a company or government agency reaches out to you asking for personal information, type in their web address directly into your browser, get their email address or phone number, and contact them directly. If it turns out that the original request was erroneous, then report it to that organization. Additionally, if a link strikes you as suspicious, you can go to the organization’s website to see if you can obtain information directly from the source (i.e., don’t click on the link provided to you an email, don’t copy and paste a web address, rather type it in directly).

**Four Steps to Protect Yourself Online**

While you may take multiple actions to safeguard your personal information online, the four steps below may assist you in

**1. Protect your computer and router by using security software (e.g., virus scanners, firewalls, secure communications)**. Set the software to update automatically so it can deal with any new security threats.

**2. Protect your devices and configure your online accounts.** These updates could give you critical protection against privacy and cyber security threats. Additionally, check your privacy and security settings on all devices and online accounts from time to time to help make sure they are in line with your preferences.

**3. Protect your accounts by using multi-factor authentication.** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you know – like a passcode you get via text message or an authentication app.
- Something you are – like a scan of your fingerprint, iris scan, or your face.
- Something you have – like a smart card.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

**4. Protect your data by backing it up.** Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or a reputable cloud storage service. Back up the data on your phone, too.

## How to Protect Yourself Against Scams and Recourse for Victims

**What to Do If You Fell Victim to a Scam:**

If you think a scammer has your personal information, such as, your Social Security Number, credit card details, or bank account number, go to IdentityTheft.gov. There you'll see specific steps to take based on the information that may have been compromised.

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your home computer or device security software immediately. Then run a scan. Check your privacy and security settings.

**Report Suspected Phishing**

If you received a personal email or text message that was fraudulent, report it.

**Step 1.** If you got a phishing email to your personal email, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org. For phishing texts, forward it to SPAM (7726).

**Step 2.** Report the phishing attack to the FTC at: ftc.gov/complaint.
*(How to Recognize and Avoid Phishing Scams, FTC)*

## Additional COVID-19 Scams Resources

- FTC Scam-Alerts
- U.S. Dept. of Justice: The Virginia Coronavirus Fraud Task Force
- The Cybersecurity and Infrastructure Security Agency (CISA)
- COVID-19 Security Resource Library