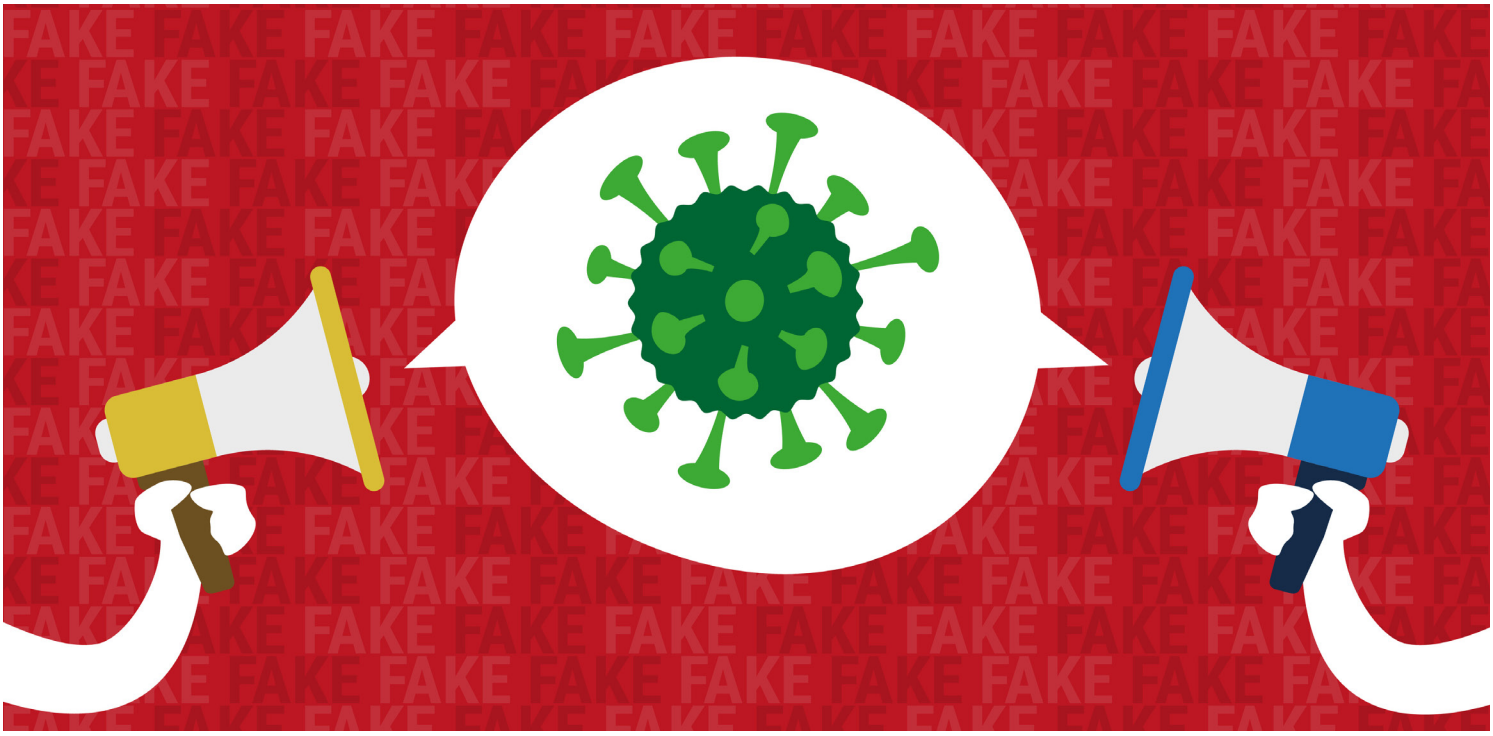
Coping with COVID-19

Steering clear of pandemic-related scams



Scam artists are always looking for ways to make a quick, dishonest buck; a crisis like COVID-19 makes it even easier for hucksters to exploit trusting people. This publication highlights some of the most common types of scams related to the pandemic, helps you spot and avoid a scam, and tells you where to report scam attempts.

Pandemic-related scams

The number of annual scam cases had already been on the rise, but the coronavirus pandemic gave con artists many new opportunities to cheat consumers (*https://www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html*), including:

Financial assistance: Aware that many people have had trouble making ends meet due to pandemic-related unemployment and underemployment, con artists have posed as sources of aid and assistance to trick victims out of money or personal information (that could be used to commit financial fraud). Mortgage relief has been one angle, with crooks offering homeowners in trouble "help" by promising to pay off their mortgage (and avoid foreclosure) and allowing them to rent and/or eventually buy the house back from the scammer. In reality, the scammer pockets the rent money—without paying the mortgage—until foreclosure proceedings result in eviction.

COVID preventives and cures: Scams directly related to combatting the virus have included the sale of counterfeit (or nonexistent) N95 masks, fake COVID-19 tests, wacky and ineffective "cures" (including a stem cell "jelly" injection that supposedly reverses lung damage from COVID-19), and spots on a vaccine "waiting list."

Employment: The pandemic has provided scammers peddling work-from-home schemes the perfect opportunity for fraud: a huge pool of unemployed/underemployed workers; a new,

widespread acceptance of remote work; and the perfect reason (quarantine) to explain why the "employer" doesn't want to meet the applicant in person. Promising easy work and high earnings, these cons often require jobseekers to fork over hundreds or thousands of dollars for "training" or other new-hire expenses. Some trick "hires" into processing transactions with stolen funds from other victims in order to launder the criminal's "earnings" and evade law enforcement.

e-Commerce: With so many people buying online because of shutdowns and quarantine, or trying to sell their stuff to generate some cash, scammers have had a lot of opportunities. Some have sold buyers non-existent toys, cars, and even puppies. Bogus texts, emails and phone calls regarding package deliveries or pending refunds have helped crooks collect phony fees or steal shoppers' personal or financial information so they can make unauthorized purchases using the stolen information. Fake check scams conducted through peer-to-peer sales sites like Poshmark, OfferUp and Craigslist have resulted in sellers losing money, and, in some cases, the item they were selling.

These are just a few of the ways scammers have exploited the pandemic for personal gain. Con artists love a crisis because they know that people let their guard down out of confusion, hope or desperation.

Spotting a scam

If you can recognize the signs of a scam, you can avoid becoming a victim. Not every scam raises all these warning signs, but all raise at least one—and they will be here long after the pandemic becomes a bad memory.

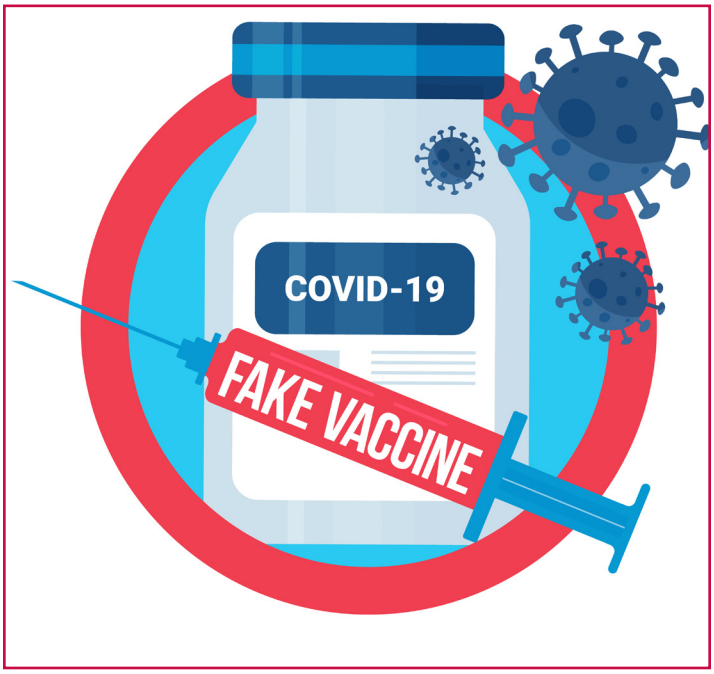
An unexpected contact: Scammers don't wait for their victims to come to them—they actively seek them out. If you're not expecting a call, email, text message or visit from a business, government agency, law enforcement officer, retailer, prospective employer, etc., the communication you receive is probably a scam attempt. Even if the person has some accurate information about you, the data could have been taken off the internet or acquired through a data breach.

A request for money or personal information: The goal of most scams is to get you to hand over your money or your sensitive information. If you get an unexpected request for either, be on alert for a scam. Scammers don't always ask for what they want outright—they cloak their requests in seemingly legitimate transactions—so don't let your guard down.

A sense of urgency: Being rushed (to hand over your money, give personal information or make an important decision) usually means someone doesn't want to give you time to do some research, verify the communication/request and make an informed decision—often the sign of a scam.

A threat or an enticing offer: Scammers get their victims to pay them or give them information by playing on their emotions—typically fear (threats of arrest, deportation, loss of account access, etc.) or hope (promises of easy money, romance, a solution to a financial problem, that sold-out toy, an early vaccine, etc.).

Demand for a particular method of payment: Crooks don't want you to be able to get your money back after you realize you've been scammed, and they don't want police to be able to track them down, so they typically request payment in the form of a wire transfer, peer-to-peer payment app transfer, prepaid card number, gift card, cryptocurrency (like bitcoin) or



other unrecoverable method, or they pay you with a fake check or a stolen credit card and request money back, saying they overpaid for one reason or another.

Unprofessional communications: Messages sent by a known business or agency that contain typos, unusual capitalization, non-native English use, bad grammar and other errors are almost certainly not legitimate. Look closely at the email address, phone number or website address (URL) provided in a communication from a known business or agency. If it doesn't match the contact information found on that company's legitimate website, your account statement or another valid source, it could be a scam attempt. (Learn about "phishing" scams at Phishing.org [https://www.phishing.org/], a site aimed at IT professionals, but educational for individuals too.)

Avoiding a scam

Here are some tips for evading a scam attempt.

Be on guard. View every unsolicited effort to reach you by someone you don't know with extreme skepticism. Credit card issuers, banks and other financial institutions, retailers, "tech support," Medicare, the CDC, Immigration Services and other government agencies will never call, email or text you and ask you to disclose your password, account number, Social Security number or other sensitive information. Unless you are receiving the communication in response to one that you initiated, it's probably a scam. Likewise, calls, emails and texts with ransom demands, blackmail attempts and claims that you need to pay to get out of legal trouble (for example, because your identity has been used to launder money or traffic drugs) are scams. Sending overdue or astronomical "invoices" to compel you to click attachments that download computer "malware" is another common ploy. Even if the communication appears to be from a legitimate source, technology has made it easy for scammers to hide or forge email addresses, block caller ID or falsely display a name or number you are likely to recognize and trust, and create lookalike URLs and copycat websites. (How-To Geek explains how to find out the real sender by digging into the email's "headers" [https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/]. Techwalla explains how to recognize fake URLs [https://www.techwalla.com/articles/how-to-recognize-a-fake-url].) If you don't want to ignore the communication because you think it might be legitimate, verify it (for example, by contacting the supposed sender at a phone number, website or email address you know to be legitimate).

Slow down, and get a second opinion. Much of scammers' success is owed to victims' hasty reactions because the scammer has intentionally created a sense of urgency. The more you feel that you must act immediately, the greater the likelihood you're dealing with a scammer. When uncertain about a request (or demand) for money, personal or account information, or access to your computer, get input from someone you can trust —a savvy friend or family member, an attorney, someone with your bank, credit card issuer or lender, a government agency employee (the CFPB, FTC, etc.), or a nonprofit consumer protection organization.

Don't 'pay to play.' Some things in life really are free—COVID vaccines, mortgage relief and other types of assistance from your creditors and service providers, grants and scholarships, a legitimate job with a legitimate employer, a prize or inheritance, etc. If you have to pay an upfront fee (or "taxes," etc.), it's almost certainly a scam. This FTC webpage tells you what next steps to take if you've paid a scammer, depending on how you made payment (https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed). (While most victims don't get their money back, the sooner you act, the better your chances for recovery.)

Limit your potential losses. When you do pay for something, use a credit card. Credit cards offer strong consumer protections under federal law—the right to dispute a fraudulent transaction, for example, and a $50 limit on your liability for unauthorized charges—and payments are traceable. Frequently check your financial account activity online for signs of fraudulent activity. If you find an unauthorized transaction, notify the bank or card issuer immediately.

Use the internet. The internet is a powerful tool for researching individuals and businesses, verifying facts and stories, checking ratings and reviews, comparing prices, and accessing scam-

fighting tips and resources. For example, doing an online search using a short description of the scheme you've been approached with can reveal if it's a widespread scam. And a reverse image search (https://www.cnet.com/how-to/google-reverse-image-search-for-your-phone-or-browser-how-to-do-it-and-why/) can help you determine if the photo of the puppy for sale was taken from some other website or if the profile picture for your latest love interest belongs to someone else. You can stay on top of the latest scams by subscribing to e-newsletters like *SCAM GRAM* (https://www.consumer-action.org/news/scam-gram), visiting websites (https://fraud.org/) and signing up for alerts (https://www.consumer.ftc.gov/features/scam-alerts) that share scam-related news, helping you develop a "sixth sense" for spotting fraud.

Report scams

Reporting a scam can help stop the perpetrators and prevent other consumers from falling for the con.

- The Federal Trade Commission (FTC) is the main agency that collects scam reports. Report your scam online at ReportFraud.ftc.gov (https://reportfraud.ftc.gov). Learn more about where to report specific types of scams at the USAGov's "Report Scams and Frauds" webpage (https://www.usa.gov/stop-scams-frauds).
- Notify your state consumer protection office of scam attempts (https://www.usa.gov/state-consumer).
- You can file a complaint about any type of fraud with the National Consumer League's Fraud.org (https://secure.nclforms.org/nficweb/OnlineComplaintForm.aspx).
- In addition to alerting the public to pandemic-related schemes (https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/), the U.S. Department of Health and Human Services encourages consumers to report COVID-19 healthcare fraud online (https://oig.hhs.gov/fraud/report-fraud/) or by phone (800-HHS-TIPS [447-8477]).
- The Better Business Bureau wants you to let them know about shady businesses and questionable offers using their BBB Scam Tracker (https://www.bbb.org/scamtracker/reportscam).
- Report fake websites, emails, malware and other internet scams to the Internet Crime Complaint Center (IC3) (https://www.ic3.gov/).
- Some scams originate outside the U.S. Report international scams to econsumer.gov (https://www.econsumer.gov/FileAComplaint#crnt).

Consumer Action guides

Just Say No to Scams: A guide to protecting yourself from liars, cheats and crooks (https://www.consumer-action.org/modules/articles/scams_guide)

Common Scams: Recognizing and avoiding fraud (https://www.consumer-action.org/modules/articles/common_scams)

Just Say No to Scams (Quick Tips) (https://www.consumer-action.org/modules/articles/scams_tip_sheet)

Coping with COVID-19: Avoid pandemic-related ID theft and account fraud identifies some pandemic-related schemes, offers tips for safeguarding your data, explains how to detect fraud and ID theft, and outlines the steps to take if you discover you're a victim (https://consumer-action.org/english/articles/id_account_theft_covid).

About Consumer Action

www.consumer-action.org

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

Consumer advice and assistance: Submit consumer complaints to: https://complaints.consumer-action.org/forms/english-form/complaint_form/ or 415-777-9635. (Spanish-language complaints can be submitted to: https://complaints.consumer-action.org/forms/spanish-form/.)

Our hotline accepts calls in Chinese, English and Spanish.

This guide was created as part of Consumer Action's COVID-19 Educational Project.

WELLS FARGO

Funding provided by Wells Fargo.