COVID-19 & SCAMS

The U.S. Department of Health and Human Services (HHS) Office of Inspector General is alerting the public about fraud schemes related to the novel coronavirus (COVID-19). Scammers are using telemarketing calls, text messages, social media platforms, and door-to-door visits to perpetrate COVID-19-related scams.

Protect Yourself

- Do not buy fake vaccine cards, do not make your own vaccine cards, and do not fill-in blank vaccination record cards with false information.
- As volunteers go door-to-door to inform communities across the country about COVID-19 vaccines, be sure to protect yourself from criminals who are seeking to commit fraud. Do not provide personal, medical, or financial details to anyone in exchange for vaccine information and obtain vaccinations from trusted providers.
- Offers to purchase COVID-19 vaccination cards are scams. Valid proof of COVID-19 vaccination can only be provided to individuals by legitimate providers administering vaccines.
- Be cautious of COVID-19 survey scams. Do not give your personal, medical, or financial information to anyone claiming to offer money or gifts in exchange for your participation in a COVID-19 vaccine survey.
- Photos of COVID-19 vaccination cards should not be shared on social media. Posting content that includes your date of birth, health care details or other personally identifiable information can be used to steal your identity.
- Beneficiaries should be cautious of unsolicited requests for their personal, medical, and financial information. Medicare will not call beneficiaries to offer COVID-19 related products, services, or benefit review.
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies. If you receive a suspicious call, hang up immediately.
- Do not respond to, or open hyperlinks in text messages about COVID-19 from unknown individuals.
- Ignore 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.
- Do not give your personal or financial information to anyone claiming to offer HHS grants related to COVID-19.
- Be 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.
ONLINE SHOPPING PROTECTION

Shopping online? Know your retailer and your rights

According to the Federal Trade Commission (FTC), COVID opened the door for scammers to double down on their worst practices, while preying on consumers during an unprecedented global pandemic. That includes some bad actors who have been taking advantage of online shoppers in search of hard-to-find items like face masks and other personal protective equipment.

When you shop online, sellers are supposed to ship your order within the time stated in their ads, or within 30 days if the ads don’t give a time. If a seller can’t ship within the promised time, it has to give you a revised shipping date, with the chance to either cancel your order for a full refund or accept the new shipping date.

So, before you shop online, especially from an unfamiliar retailer, remember these three things:

1. Check out the company or product. Search online for the name plus terms like “review,” “complaint,” or “scam.” See what other people say about it. Read the seller’s description of the product carefully. If the seller has name-brand goods at steeply discounted prices, they might be fakes.

2. Look at the terms of the sale. Make note of the total price, including taxes, shipping, and handling; the expected delivery date; and policies for refunds, including who pays for return shipping and if there is a restocking fee.

3. Pay by credit card. You’ll get protections under federal law, so you don’t have to pay for things you ordered but did not get.

The FTC has also warned consumers about scams involving fake Amazon representatives. Has Amazon contacted you to confirm a recent purchase you didn’t make or to tell you that your account has been hacked? According to the FTC, since July 2020, about one in three people who have reported a business impersonator scam say the scammer pretended to be Amazon.

In one version of this scam, scammers offer a “refund” for an unauthorized purchase but “accidentally transfer” more than promised. They then ask for the difference to be sent back. What really happens? The scammer moves a victim’s money from one of their bank accounts to the other (like Savings to Checking, or vice versa) to make it look like they were refunded. Any money you send back to “Amazon” is your money (not an overpayment) and as soon as you send it out of your account, it becomes theirs. In another version of the scam, victims are told that hackers have gotten access to their account, and the only way to supposedly protect it is to buy gift cards and share the gift card number and PIN on the back. Once that information is theirs, the money is, too.

Here are some ways to avoid an Amazon impersonator scam:

- **Never call back an unknown number.** Use the information on Amazon’s website and not a number listed in an unexpected email or text.

- **Don’t pay for anything with a gift card.** Gift cards are for gifts. If anyone asks you to pay with a gift card or buy gift cards for anything other than a gift, it’s a scam.

- **Don’t give remote access to someone who contacts you unexpectedly.** This gives scammers easy access to your personal and financial information—like access to your bank accounts.
HAVE YOU BEEN SCAMMED?

If you've been scammed online, the person who stole your information can wreak havoc on your life. Regardless of what's been taken from you, it's crucial to take steps to protect yourself as quickly as possible. That includes contacting your creditors and the credit reporting agencies, as well as filing a report with the Federal Trade Commission (FTC) and your local police department. Learn about these steps and how they can help you stop identity thieves in their tracks.

Contact Your Banks and Credit Card Companies
If the scam involved your credit card information or login credentials for your financial accounts, contact your banks and credit card companies immediately to cancel your cards and receive new ones.

While you're getting help with this process, ask the representative to check your recent transactions to make sure you recognize them. If there are some that you don't, you can flag them as fraudulent.

Also, take some time to change your online passwords to stop the criminal from accessing your accounts. If you use the same password on more than one website, update each account with a unique password to make it more difficult for hackers to crack.

If you have many different passwords and need help keeping track of them, consider registering for a password manager like LastPass or 1Password.

Reach Out to the Credit Bureaus
If you think someone has obtained your personally identifiable information, especially your Social Security number, contact each of the credit bureaus to restrict access to your credit reports.

Submit a Complaint to the Federal Trade Commission
Submit a report about the theft to the FTC. As you go through the process, you'll answer some questions about what happened, and the FTC will create a personal recovery plan to help you with the next steps.

File a Police Report
The process for filing a police report can vary depending on where you live. Check with your local law enforcement agency to see if you can file a report online or if you need to submit a report in person. Go through the report and answer all the questions to the best of your ability. After you've filed the report, request a copy of it, especially if you're thinking about requesting an extended fraud alert on your credit reports. Source Experian.com
HOW TO REPORT WORKPLACE FRAUD

The Florida Department of Elder Affairs Office of Inspector General is a resource for employees, contractors and subcontractors related to fraud in the workplace.

The Office of Inspector General (OIG) encourages all employees, contractors, and subcontractors to report any suspected fraudulent activity. If possible, report incidents of suspected fraudulent activity to your supervisor.

If you are unable to report the suspected fraudulent activity to your supervisor, you can notify the Office of Inspector General via email at OIG@elderaffairs.org or by calling 850-414-2311.

All reports of suspected fraudulent activity will be reviewed and may or may not rise to the level of an investigation.

Office of Inspector General Contacts:

Inspector General Taroub J. Faraj Office (850) 414-2013
Email- farajt@elderaffairs.org

Director of Internal Audits Kimberly Jones
Office (850) 414-2117
Email – jonesk@elderaffairs.org

Inspector Mark Meadows Office (850) 414-2311
Email – meadowsm@elderaffairs.org

Internal Auditor Shumikia Duval (850) 414-2173
Email – Duvals@elderaffairs.org