Scams Are on the Rise

Protect yourself from financial fraud during the pandemic.

LIKE MANY OTHER AMERICANS, YOU MAY BE EAGERLY AWAITING YOUR STIMULUS CHECK. Perhaps you've been checking to see if it's shown up in your mailbox or bank account. And maybe you've received a call from someone claiming to be from the IRS who promised to get your check to you faster.

You can probably trust someone calling and claiming to be from the IRS, right?

The correct answer is no! There is a new wave of scammers who are using clever tricks to take advantage of people during this global pandemic. They're using a variety of methods such as posing as the IRS or offering to sell you phony test kits, among other devious scams.

Americans are not new victims to fraud, but the coronavirus has opened the floodgates to a whole host of new scams this year. In 2019, scams took an estimated $1.9 billion away from Americans, and 74% of reported fraud began with a phone call, according to the Federal Trade Commission (FTC). The FTC says phone-based scams stole nearly $493 million, while online fraud took $325 million. Email-based schemes accounted for another $226 million.[1]

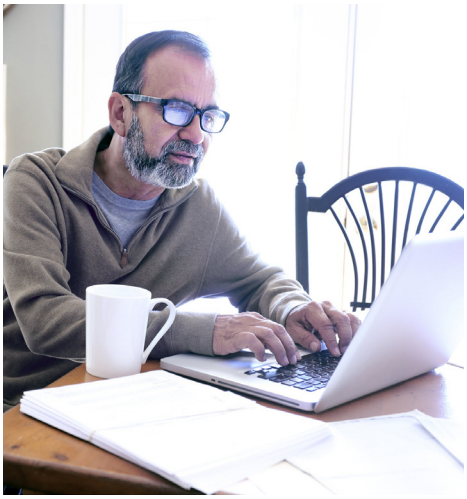
Victims aren't always the stereotype painted for us—a naïve, absent-minded centenarian. It could just as easily be any of us. The sad truth is that many of those who get taken advantage of are unknowingly willing participants. They simply don't have the training to spot when they're being taken advantage of by a scammer.

Bad Guys Are Real

Attackers. Bad actors. Malicious users. No matter what you call those trying to scam you, they're certainly not good guys. Worst of all, these callous criminals are becoming more sophisticated. With additional data about you from multiple sources—including social media—floating around the web, it's not out of the ordinary to get an unsolicited phishing email that passes for a legit communication. They know more info about you than you may suspect.

More often than not, they're trying to get you to do something. Click, call, or reply. Is some unknown person coming into your life asking for something? Be skeptical. Even a quick survey can turn into a thorny trap.

With an online interaction or a phone call, people tend to let their guard down. They're more inclined to do the requested action because there's an inherent level of trust on a computer or phone that's not there if asked in person. The misconception is the email can only come from whom it says it's coming from.



Key Points

- Financial scams—conducted over the phone and online—can rob unsuspecting Americans of millions of dollars each year.
- Many victims of financial fraud are willing participants who do not know they are being taken advantage of until it's too late.
- Stop and question the validity of any stranger requesting you take an action that may involve your identity or finances.

[1] "Consumer Sentinel Network Data Book 2019," FTC, 1/20

Be Alert When You Receive an Alert

Here's a three-step action plan to think through for the next time you get an unsolicited email or phone call:

1. **Stop**—Don't just jump in and open any email or answer any phone call. Take a timeout.
2. **Think**—Does it make sense? Are you expecting an email communication or call?
3. **Protect**—Verify the sender. Once you open an email or pick up the phone, investigate whether the person is asking you to do something. If you're still confused, call back the individual or organization with a number you have from a business card, the back of a credit card, or from an official website.

Here's a specific example:

You receive an email from the U.S. Centers for Disease Control (CDC). It might inform you of a new healthcare response to the coronavirus, or it might have attachments regarding new measures that you should take to stay safe. Following the link may prompt you to enter your email address to access the information. The communication looks like it's from the CDC. It has the look and feel of an email from a professional organization, and the email domain from which it's sent looks correct.

It should be safe to click through, right?

As it turns out, the email's not from the CDC at all. It's from the bad guys. They've put the login page on what's called a phishing site—a site that's designed to steal your information. You log in, and now they have your information. The same trick can happen over the phone. Phone numbers on caller ID can be spoofed, too. In fact, scammers are now calling from numbers that look like they're local. They know you're more likely to answer if you recognize the area code.

The bottom line: Don't trust anyone—even someone claiming to be from a place as reputable as the CDC. Don't willingly share personal information over the phone. Verify the identity of anyone asking you for anything. Then take the time to process it. You probably don't have all of the facts. Do a quick Google search to determine as much as you can while speaking with them. Why are they reaching out to you in the first place?

(See a list of common scams on page 3 for more scenarios.)

Victims Come in All Shapes and Sizes

People think fraud can't happen to them. We often don't realize that being scammed is a very real possibility until somebody close to us falls victim.

Seniors aren't the only victims, but they are the prime targets since they tend to be less comfortable working with newer technology. This creates an opportunity for scammers to take advantage of that lack of comfort.

Unfortunately, the public receives virtually no training on how to deal with these situations. So, there's little awareness of what to do. And this threat isn't going away any time soon. Defend yourself from being a victim.

Learn how to take shelter from financial fraud—in whatever form it may come. And in the time of coronavirus, be especially vigilant against new scammers who are looking to take advantage of vulnerable and panicked victims.

Avoid Coronavirus Scams

- **Don't respond to texts, emails, or calls about checks from the government.** The IRS will never request personal information from you through calls, texts, or emails.
- **Ignore online offers for vaccinations and home test kits.** There are no products proven to treat or prevent COVID-19 at this time.
- **Hang up on all robocalls.** Scammers are using illegal robocalls to pitch everything from low-priced health insurance to work-at-home schemes.
- **Watch for emails claiming to be from the Centers for Disease Control (CDC) or the World Health Organization (WHO).** Use sites such as coronavirus.gov and usa.gov/coronavirus to get the latest information. And don't click on links from sources you don't know.
- **Do your homework when it comes to donations.** Never donate in cash, by gift card, or by wiring money.

Source: Federal Trade Commission

Other Common Scams To Be Aware of Today

Here's a compilation of the biggest schemes perpetrated on Americans. Learn the various methods used and how you can best prevent becoming a victim.

1. **Census Bureau phone call scams**
   While these calls are often legitimate and can happen year-round, it's best to call the US Census Bureau to confirm that it's real rather than giving personal info out on the phone.
2. **Medicare scams**
   Perpetrators may pose as a Medicare representative to obtain personal information.
3. **Counterfeit prescription medicines**
   Cheap prescription drugs online, where seniors increasingly go to find better prices, are often bogus counterfeit medications.
4. **Funeral home and cemetery scams**
   Money is extorted from relatives of the deceased to settle fake debts. Disreputable funeral homes could capitalize on unfamiliarity by adding unnecessary charges to the bill.
5. **Fraudulent anti-aging products**
   Scams of this nature target seniors with bogus (and costly) anti-aging treatments that often do nothing at all.
6. **Telemarketing/phone scams**
   These scammers can call from anywhere in the world and are now spoofing to local numbers to seem more legitimate. They are often trying to get personal information to use or sell later.
7. **Internet fraud**
   Scammers will often prey on unfamiliarity and skill deficits of older internet users, making them fall victim to email or phishing scams, pop-ups, or virus protection scams.
8. **Investment schemes**
   Bad guys—posing as financial advisors—gain access to retirement funds and savings, take money, and then disappear.
9. **Homeowner/reverse-mortgage scams**
   Seniors are pressured to take out equity in their home to use as payment for reported necessary repairs.
10. **Sweepstakes and lottery scams**
    Seniors are contacted to inform them that they've won a financial prize, but are required to advance payment of a fee to collect the winnings.
11. **The grandparents scam**
    Scammers pose as grandchildren and ask for money to solve some unexpected financial problem. Or, someone calls on behalf of a grandchild who is either (fictionally) in jail, a hospital, or another country.
12. **Tech support**
    A fake technical-support representative calls to fix a nonexistent computer issue with the goal of gaining remote access to a victim's computer.
13. **IRS impersonation**
    Victims are told they're due a tax refund or that they have unpaid taxes. The IRS will never initiate contact via phone calls, email, or through social media.

Sources: ABC, IRS, FTC, and National Council on Aging