

COVID SCAMS

The coronavirus pandemic has created a world of new opportunities for fraudsters. During this time of increased isolation, older Americans are more at risk than ever for being the victim of fraud or identity theft. Below, are some resources for protecting yourself and your loved ones from COVID-19 scams:



Phishing Scams

The goal of a phishing scam is to collect personal information from you online, over the phone or in a text message. Often these communications appear to come from a real business or government agency. Be skeptical, especially if they are sent to you unsolicited.

During COVID-19, illegitimate contact tracing messages can be another route for scammers. If a contact tracing message includes a link for you to click, **do not click it**. Legitimate contact tracers working for public health agencies will not include a link or ask you for money or personal information. Clicking on these links can result in downloading malware to your device, which can find passwords and other information used for identity theft.

Never provide your Social Security number, Medicare number, bank account information, or credit card information to anyone who contacts you unsolicited.

SPOTTING COMMON SCAMS



Disinformation

Make sure what you're reading and sharing is accurate and coming from a trustworthy source. Spreading false information, especially about a global health crisis, can be life-threatening.



Treatments/Cures

There are no approved treatments, cures, or vaccines for COVID-19 yet. Ignore any online offers for medicines or devices that claim to treat or cure COVID-19.

A real medical breakthrough will be reported by major news outlets and government agencies.



Fake Charities

Fake charities have cropped up during the pandemic and will solicit donations but not use them for the purpose you were given. Before donating, research the charity using one of the organizations listed at www.ftc.gov/charity.



Government Aid Checks

The government won't contact you for a Social Security number, bank account or credit card number to give you a stimulus payment—or ask you to pay anything up front.



Robocalls

If you receive a robocall, hang up. Do not press any buttons. Some robocalls claim to be from the IRS but the IRS will never call you to demand payment by debit card or wire transfer, threaten immediate arrest, or ask you to make payment to anyone other than the U.S. Treasury.

How to spot if your loved one is a victim of a scam

It's not always obvious when someone has been the victim of a scam, and physical distancing makes it even more important to be vigilant in the ways that we can. Victims of a scam may also be embarrassed or uncomfortable asking for help. Check in frequently with your loved ones, especially if they are older, live alone, or you have other reasons to feel they may be at higher risk.

Warning Signs Include

- Large ATM withdrawals, charges on credit cards, or checks
- Secretiveness or unusual anxiety, especially about finances
- Large quantities of goods being delivered that they don't need
- An unusual number of phone calls or visits from strangers
- A sudden lack of money, unpaid bills, or a change in daily habit

Get help at:
www.ftc.gov/coronavirus or www.cdc.gov/coronavirus/2019-ncov