While most of us are focused on staying safe during this crisis, we need to be wary of bad actors who are using this pandemic for their own financial gain. This week, I want to alert you to the danger of coronavirus-related scams and provide you with some information for keeping your information secure.

Scams in the age of COVID-19 can take a variety of forms. Here are a few examples:

* Advanced fee schemes, through which scammers ask for money up front for goods (masks, protective equipment, hand sanitizer) or services (COVID-19 tests);
* Counterfeit products, like knock-off N-95 masks that don’t actually work;
* Impersonation of government officials demanding payment;
* Investment schemes that falsely promise you the chance to profit off the pandemic;
* Solicitations for private information, such as your Social Security Number, bank account number, or Medicare/Medicaid number;
* In-person marketers offering free COVID-19 testing; and
* Fake phone calls from the IRS offering to help you get a stimulus payment.

If you’ve already given out personal or financial information, you should check and freeze your credit reports, change your passwords and account information, and monitor your finances for unexpected changes.

Various agencies and organizations have released consumer alerts regarding specific scams that have been reported. You can follow these links to find alerts from the [Florida Attorney General,](https://shalala.house.gov/components/redirect/r.aspx?ID=721-500340) the [Federal Trade Commission (FTC)](https://shalala.house.gov/components/redirect/r.aspx?ID=722-500340), the [Federal Communications Commission (FCC),](https://shalala.house.gov/components/redirect/r.aspx?ID=723-500340) and the [Better Business Bureau](https://shalala.house.gov/components/redirect/r.aspx?ID=724-500340).

Fortunately, you can foil these schemes by staying vigilant. Check out these tips for avoiding coronavirus-related scams:

* Don’t respond to texts, emails, or calls about checks from the government. Government agencies will never call you to ask for personal information or money.
* Never share personal or financial information via email, text, or over the phone.
* Ignore online offers for vaccinations. There are no products proven to treat or prevent COVID-19 at this time. Check with medical professionals before purchasing an unproven health product.
* Be wary of ads for test kits. While the FDA recently announced approval for one home test kit, which requires a doctor’s order, most test kits being advertised have not been approved by the FDA and do not provide accurate results.
* Hang up on 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 CDC or WHO. Use sites like [coronavirus.gov](https://shalala.house.gov/components/redirect/r.aspx?ID=725-500340) and [usa.gov/coronavirus](https://shalala.house.gov/components/redirect/r.aspx?ID=726-500340) to get the latest information. Don’t click on links from sources you don’t know; these links can download malware onto your computer.
* If malware is suspected, do not shop online, access online banking or do other activities that involve sensitive information like usernames, passwords, or account information until it has been checked out by a trusted technical support provider.
* Only buy products from reputable stores and websites. Be sure online stores have working contact information. Before offering up personal information, make sure the store has a real street address and working customer service number.
* Research before donating. Search for the charity’s name online, using the words scam or complaint, and check resources for information about the charity, such as [Charity Navigator](https://shalala.house.gov/components/redirect/r.aspx?ID=727-500340) and the Better Business Bureau’s Wise Giving Alliance at 1(703) 247-9321. Never donate in cash, by gift card, or by wiring money.

If you encounter scams, you should report them. You can use the [FBI tip site](https://shalala.house.gov/components/redirect/r.aspx?ID=728-500340), the [Internet Crime Complaint Center](https://shalala.house.gov/components/redirect/r.aspx?ID=729-500340), or the [Florida Attorney General’s website](https://shalala.house.gov/components/redirect/r.aspx?ID=730-500340) to help prevent other people from falling victim to scams. You can also call the Florida Attorney General’s Fraud Hotline at (866) 9-NO-SCAM or (866) 966-7226.