



Protect yourself from COVID-19-related scams

Criminals are coming up with new ways to prey on our emotions and vulnerabilities.

With people isolating due to the spread of COVID-19 and anxiety running high, criminals are trying to take advantage of the uncertainty and confusion. From dangerous fake cures to government relief scams, knowing how to protect yourself and your loved ones is critical. Here are some common scams related to the COVID-19 pandemic:

Fake emails, texting and phishing

Scammers use fake emails and texts, often disguised as legitimate agencies or companies, in an attempt to get you to share your valuable personal information, such as your Social Security number or financial account numbers. Phishing emails and websites also lure you to click and download ransomware or malware to your computer so fraudsters can steal your information through online channels.

Government assistance/ stimulus/relief scams

These scams involve texts, emails and phone calls claiming to facilitate relief or stimulus programs, loans and government assistance in an effort to obtain your personal information or ask you to prepay associated fees. Only rely on trusted sources for this information, such as [irs.gov](https://www.irs.gov), and know that you never have to pay a fee to receive government assistance.

Vaccine and treatment scams

Fake tests, treatments and cures for the coronavirus and the disease it causes, COVID-19, are all over social media. Don't take the bait. Use reputable information from the CDC and seek medical testing and treatment from a physician if you feel ill.

Home sanitation scams

These scams offer HVAC cleaning and general sanitation as a way to protect your home from the virus. These types of services are not an effective way of protecting yourself from exposure to or contracting the virus. Scammers are also offering to ship sanitation supplies and kits overnight and don't deliver the goods.

Charitable giving scams

Fake charities and phony organizations have emerged with the promise of helping those in need. Before you make a donation, always verify that the charity or company is legitimate. Reliable sources of information include www.guidestar.org and www.ftc.gov/charityfraud.

Investment scams

Scammers offer too-good-to-be-true investment schemes and flood the marketplace with inaccurate information in an attempt to manipulate markets and investors. They often claim research and development opportunities or medical breakthroughs in pop-up ads and through social media.

Steps to protect yourself

- Do not answer calls from unknown numbers and immediately hang up on robocalls. Do not follow any prompts or wait to speak to someone to add yourself to their do not call list. To stop receiving cold calls, add your name to the National "Do Not Call" Registry at (888) 382-1222 (TTY: (866) 290-4326) or online at www.donotcall.gov.
- Refuse to share sensitive information or make a payment to someone calling you.
- Don't click on links or open attachments from sources you don't recognize.
- Confirm your computer and other electronic devices have the most recent security and software updates.
- Do your homework when it comes to charity donations and always pay by credit card. Don't use gift cards or wire transfer.
- Ignore internet and phone offers of new treatments and cures and instead rely on advice from the CDC or your physician.

Knowledge is power

Con artists tend to target older Americans because they are more likely to have financial assets. In addition, many physical and emotional conditions due to aging can make older Americans more susceptible to fraud and exploitation. As always, at RBC Wealth Management, helping you protect your finances is a top priority.

In addition to providing you with information about changing trends in financial exploitation, we are increasing our efforts to protect you from these trends. If you have any immediate concerns, please call your financial advisor.

Additional resources

- The Centers for Disease Control and Prevention provides up-to-date health information regarding the COVID-19 pandemic at [cdc.gov/coronavirus](https://www.cdc.gov/coronavirus).
- The Federal Trade Commission provides an extensive library of educational content about fraud protection and filing a complaint at www.ftc.gov or [ftc.gov/coronavirus](https://www.ftc.gov/coronavirus).
- The Financial Industry Regulatory Authority offers fraud prevention information and resources at www.finra.org/investors/avoid-fraud.
- The Securities and Exchange Commission has a wealth of practical consumer awareness information at www.sec.gov/investor/pubs.shtml.
- For more information contact your financial advisor.

Having a trusted contact person is important

At RBC Wealth Management, if we think you may be a victim of fraud, we will contact you. Fast action can help resolve issues quickly. A trusted contact person is someone you authorize us to contact if we are unable to reach you directly. This person should be someone you trust, such as a family member or friend, or a professional you depend on, like an accountant or attorney.

Your trusted contact person will not be an authorized party on your accounts, and details about your account will not be shared with them. It's simply another way for us to reach you if we need to.

To add a trusted contact person to your account, contact your financial advisor with their name, address and phone number.