



# Cyber Section

## Tips to Avoid Coronavirus Financial Scams, Investment Schemes

Consumers should be wary of potential financial and investment scams related to COVID-19. Scammers will often target individuals through unsolicited communications – by phone, email, or even social media.

Spot these common characteristics of [financial scams](#):

- Sense of urgency and limited time offers
- Payment with wire transfer or gift cards
- Secrecy, request not to tell anyone
- Low or minimal risks with guaranteed high returns

“We all wish we could expect everyone to act with integrity and credibility, but too many scam artists prey on our good intentions to trust,” advises Acting Secretary Vague. “Scam artists are manipulative and all of us must remain ever vigilant. With a few simple precautions, you can help detect and prevent this from happening to you or a loved one.”

In addition to financial scams, the North American Securities Administrators Association (NASAA) anticipates a rise in [fraudulent investment schemes](#) as a result of the ongoing coronavirus outbreak.

Some hallmarks of these types of investment scams are:

- Falsely purporting to raise capital for companies manufacturing personal protective equipment, ventilators, medical equipment, or vaccines.
- Promoting “safe” investments with “guaranteed returns” including those tied to gold and other commodities; oil and gas; and real estate.
- Touting “get rich quick” schemes with quickly earned returns.
- Targeting retirees and senior citizens with false claims that they can quickly and safely recoup any losses.

Ways to protect yourself from scams and schemes:

- If it sounds too good to be true, it probably is. When in doubt, delete the email or direct message, or hang up the phone in response to unsolicited communications.
- Scam emails are made to sound and look legitimate. Never open an attachment or link from an unsolicited email.
- Never share personal or financial information without independently verifying any request.
- [Investigate Before You Invest](#). Research any financial service, professional, investment, or company before spending your time and money. Find tools and resources on the DoBS website.

## COVID-19 Characteristics of Scams

- Sense of urgency and limited time offers.** (Icon: hand holding a clock)
- Payment with wire transfer or gift cards.** (Icon: wire transfer symbol and gift card)
- Secrecy and the need to not tell anyone.** (Icon: speech bubble saying "shush! quiet!")
- Low or minimal risks with guaranteed high returns.** (Icon: "60% GUARANTEE" badge and money)
- Unsolicited offers via social media or direct communication.** (Icon: megaphone and person holding a sign)

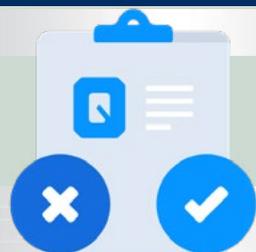


Video: [How to Identify and Avoid Investment Scams](#)

## Contact DoBS

Call **1.800.PA.BANKS** or 800.600.0007 or [online](#) to ask questions or file complaints about financial transactions, companies, or products.

If you believe you have fallen victim to a scam, contact local law enforcement through a non-emergency number.



### [Newsletter Satisfaction Survey:](#)

Take this short survey and let us know how we can improve our newsletter.



## Stimulus Payment Phishing Scams



Fraudsters may target people expecting stimulus payments from the federal government. The Pennsylvania Department of Revenue and DoBS want Pennsylvanians to know the warning signs of these [stimulus payment phishing scams](#):

- Ask you to confirm banking or personal information via phone, email, text, or social media saying it is required to speed up their economic impact payment.
- Ask you to sign over your economic impact payment check to them.
- Suggest they can help you get a tax refund or stimulus payment faster.
- Mail a bogus check, then tell the taxpayer to call a number or verify information online in order to cash it.

Protect yourself against these scams by:

- Be on the lookout for imposters.
- Approach unusual attachments and links with caution.
- Conduct research online.

[Additional information](#) regarding economic impact payments is available from the IRS.

If you are a victim of identity theft or discover a fraudulent Pennsylvania personal income tax return was filed using your identity, please contact Revenue's Fraud Detection and Analysis Unit by emailing [RA-RVPITFRAUD@pa.gov](mailto:RA-RVPITFRAUD@pa.gov).

## Tips for Pennsylvanians Receiving Paper Stimulus Checks

It is important consumers understand check cashing fees so they keep as much of their money as possible. [Check cashing fees](#) may occur for Pennsylvanians receiving their stimulus checks in paper check form instead of direct deposit.

Before cashing your check:

- Search the [NMLS Consumer Access website](#) to confirm proper license or registration of an establishment.
- Recognize that a registered retail check casher may issue a maximum fee of **1.5 percent** of the value of the check.
- Take action if an establishment charges more than **1.5 percent** by contacting DoBS immediately at [dobs.pa.gov](http://dobs.pa.gov) or call **1.800.PA.BANKS**.



Pennsylvanians receiving **paper** stimulus checks may incur check cashing fees.

To track your stimulus check and to learn more information, individuals can use the IRS online tracker [Get My Payment](#).

DoBS will ensure check casher licensees are complying with statutory provisions related to fees on government checks during ongoing examinations.

