SCHMERSAHL TRELOAR & CO.
Certified Public Accountants

COVID-19 Scams to Avoid Like the Virus

March 8, 2020

The coronavirus (COVID-19) pandemic presents the biggest challenge our country has faced in recent history. But the risks aren't only related to the health and financial issues that have been making headlines. Opportunistic con artists have exploited the situation for their own financial gain. The result? Even more financial damage for individuals and businesses. Here are six COVID-19 scams to watch out for. Crisis brings out the best – and worst – in people. Some dishonest people have already turned the coronavirus (COVID-19) pandemic to their advantage by preying on unsuspecting victims and exploiting their fears.

"History has shown that criminals take every opportunity to perpetrate a fraud on unsuspecting victims, especially when a group of people is vulnerable or in a state of need," said IRS Criminal Investigation Chief Don Fort.

Here's an overview of six COVID-19-related scams and practical advice on how to avoid them.

1. Fake Charities

When a catastrophe like COVID-19 strikes, philanthropists flock to donate cash and other assets to help relieve the suffering. But, before making a donation, be aware that opportunistic scammers may set up fake charities to benefit from your generosity.

Fake charities often use names that are similar to legitimate charitable organizations. So, be sure to do your homework before making a contribution. Donors aren't the only victims to these scams – those in need also lose out.

2. Stolen CARES Act Payments

The new Coronavirus Aid, Relief, and Economic Security (CARES) Act provides one-time direct "economic impact" payments to individuals and families. If you're eligible, these payments are up to $1,200 for single people and $2,400 for joint filers, plus $500 per qualifying child under 17. They're considered advances for a new federal income tax credit that's subject to phaseout thresholds based on adjusted gross income (AGI).

People who are strapped for cash may be impatient to receive the money – and cyber-crooks know it. Scammers may, for instance, call or email you, pretending to be from a government agency like the IRS. Then they'll ask for your Social Security number (SSN) in order to receive your check. Or they'll say you must make a payment to qualify for the check.

The IRS warns that scammers may:

- Use the words "Stimulus Check" or "Stimulus Payment." (The official IRS term is economic impact payment.)
- Ask the taxpayer to sign over their payment check to them.
- Ask by phone, email, text or social media for verification of personal and/or banking information saying that the information is needed to receive or speed up their payment.
- Suggest that they can get a tax refund or payment faster by working on a taxpayer's behalf. This scam could be conducted by social media or even in person.
- Mail the taxpayer a bogus check, perhaps in an odd amount, then tell the taxpayer to call a number or verify information online in order to cash it.

Don't fall for these ploys! If you previously signed up to have your federal income tax refunds deposited into a bank account, your advance credit payment will come to you that way. If not, you may be entitled to receive a paper check through the mail. Either way, the U.S. Treasury won't contact you over the phone or email you with a request for payment or sensitive personal data (such as a bank account or SSN).

3. Public Health Phishing

In a "phishing" scheme, victims are enticed to respond to a false email or other online communication. In COVID-19-related phishing scams, the perpetrator may impersonate a representative from a health care agency, such as the World Health Organization (WHO) or the Centers for Disease Control and Prevention (CDC). They may ask for personal information, such as your SSN or bank account, or instruct you to click on a link to a survey or an email.

If you receive a suspicious email, don't respond or click on any links. The scammer might use ill-gotten data to gain access to your financial accounts or open new accounts in your name. In some cases, clicking a link might download malware to your computer. For updates on the COVID-19 crisis, go directly to the official websites of the WHO or CDC.

The IRS reports that its Criminal Investigation Division has seen a wave of new and evolving phishing schemes against taxpayers, and among the targets are retirees.

4. Retail Scams

In some parts of the United States, there's little or no supply of certain consumable goods, such as toilet paper, hand sanitizer, antibacterial wipes, masks and paper goods. Scammers are exploiting these shortages by posing as retailers in order to obtain your personal information.

Con artists may, for example, claim to have the goods that you need and ask for your credit card number to complete a purchase transaction. Then they use the card number to run up charges while you never receive anything in return.

How can you avoid retail scams? Deal with outfits only if you know they're legitimate. If a supplier offers a deal out of the blue that seems to be too good to be true, it probably is.

In other cases, online sellers are price gouging on limited items. If an item is selling online for many times more than the usual price, you probably want to avoid buying it.

5. Robo-Calls

Robo-calls may be increasing during the COVID-19 crisis. This scam has been tailored to fit the pandemic. For instance, callers may offer masks, testing kits and other COVID-19-related items at reduced rates. Then they'll ask for your credit card number to "secure" your purchase.

A reputable company wouldn't try to contact you this way. If you receive an unsolicited call from a phone number that's blocked or that you don't recognize, hang up or ignore it.

In addition, don't buy into special offers for such items as COVID-19 treatments, vaccinations or home test kits. You'll likely end up paying for something that doesn't exist. There currently is no vaccine for COVID-19.

6. Bogus Business Emails

Businesses aren't immune to COVID-19 frauds. Frequently, scams originate from emails instructing employees to remit goods, authorize transactions or provide proprietary data.

For example, an employee might receive an email that appears to be from the company's president that directs the employee to transfer funds, wire money or take some other financial action. But the email is actually from a fraudster, hoping to steal money or gain access to the company's computer system.

Under normal conditions, this type of phishing email might have raised some eyebrows. But COVID-19 has disrupted normal business operations and caused businesses to take extreme measures to protect assets and preserve cash flow. Companies may be especially vulnerable to these scams while employees work from home and don't have the same access to management as they do during normal conditions.

Another type of phony business email appears to come from the company's IT department. These messages might ask the recipient to provide his or her password – or to download software that turns out to be malware that infects the entire system. Employees who are stressed, overworked or sleep-deprived due to COVID-19 are easy targets for this scam – especially if an employee's wireless home network is less secure than the company's in-office network.

Education is the key to avoiding COVID-19-related frauds in the workplace. Remind employees about network security protocols and phishing scams during the pandemic. And provide tools that allow them to verify any communications that seem out of the ordinary and to report hoaxes as soon as possible.

Team Effort

You're not in this alone. The Federal Trade Commission (FTC) has ramped up efforts to protect consumers on matters relating to COVID-19. Visit the FTC's website for more information about these types of scams and how to avoid them – or contact your financial advisors for additional guidance.

If you would like additional information regarding the issues presented in this bulletin please contact Schmersahl Treloar at 314-966-2727.

FTC Reports Rise in COVID-19 Scams

In the first quarter of 2020, the Federal Trade Commission (FTC) received more than 7,800 consumer complaints related to the coronavirus (COVID-19) crisis. That number is expected to surge, as the rate of complaints roughly doubled during the last week of March.

Top categories of COVID-19-related fraud complaints include:

- Reports regarding cancellations and refunds for travel and vacation plans,
- Problems with online shopping,
- Mobile texting scams, and
- Government and business imposter scams.

So far, the FTC reports that consumers have lost a total of $4.77 million from COVID-19-related frauds. The median loss is $598. If you encounter fraud related to the ongoing COVID-19 crisis, report it to the FTC.

10805 Sunset Office Dr., Ste. 400 St. Louis, MO 63127
stcpa.com / 314-966-2727