1ST SUMMIT
Financial Partners
125 Donald Lane
Johnstown, PA 15904
814-262-4040
trust@1stsummit.bank
www.1stsummit.bank

Watch Out for Coronavirus Scams

The FTC has received over 20,000 COVID-19 related complaints since January 1, 2020.

Source: Federal Trade Commission, April 2020

Fraudsters and scam artists are always looking for new ways to prey on consumers. Now they are using the same tactics to take advantage of consumers' heightened financial and health concerns over the coronavirus pandemic. Federal, state, and local law enforcement have begun issuing warnings on the surge of coronavirus scams and how consumers can protect themselves. Here are some of the more prevalent coronavirus scams that consumers need to watch out for.

Schemes related to economic impact payments

The IRS recently issued a warning about various schemes related to economic impact payments that are being sent to taxpayers under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[1] The IRS warns taxpayers to be aware of scammers who:

- Use words such as "stimulus check" or "stimulus payment" instead of the official term, "economic impact payment"
- Ask you to "sign up" for your economic impact payment check
- Contact you by phone, email, text or social media for verification of personal and/or banking information to receive or speed up your economic impact payment

In most cases, the IRS will deposit the economic impact payment directly into an account that taxpayers previously provided on their tax returns. If taxpayers have previously filed their taxes but not provided direct-deposit information to the IRS, they will be able to provide their banking information online at irs.gov/coronavirus. If the IRS does not have a taxpayer's direct-deposit information, a check will be mailed to the taxpayer's address on file with the IRS. In addition, the IRS is reminding Social Security recipients who normally don't file taxes that no additional action or information is needed on their part to receive the $1,200 economic payment — it will be sent to them automatically.

Fraudulent treatments, vaccinations, and home test kits

The Federal Trade Commission is tracking scam artists who are attempting to sell fraudulent products that claim to treat, prevent, or diagnose COVID-19. Currently, the U.S. Food and Drug Administration (FDA) has not approved any products designed specifically to treat or prevent COVID-19.

The FDA had warned consumers in March to be wary of companies selling unauthorized coronavirus home testing kits. On April 21, 2020, the FDA authorized the first coronavirus test kit for home use. According to the FDA, the test kits will be available to consumers in most states, with a doctor's order, in the coming weeks. You can visit fda.gov for more information.

Phishing scams

Scammers have begun using phishing scams related to the coronavirus pandemic in order to obtain personal and financial information. Phishing scams usually involve unsolicited phone calls, emails, text messages, or fake websites that pose as legitimate organizations and try to convince you to provide personal or financial information. Once scam artists obtain this information, they use it to commit identity or financial theft. Be wary of anyone claiming to be from an official organization, such as the Centers for Disease Control and Prevention or the World Health Organization, or nongovernment websites with domain names that include the words "coronavirus" or "COVID-19," as they are likely to be malicious.

Charity fraud

Many charitable organizations are dedicated to helping those affected by COVID-19. Scammers often pose as legitimate charitable organizations in order to solicit donations from unsuspecting donors. Be wary of charities with names that are similar to more familiar or nationally known organizations. Before donating to a charity, make sure that it is legitimate and never donate cash, gift cards, or funds by wire transfer. The IRS website has a tool to assist you in checking out the status of a charitable organization at irs.gov/charities-and-nonprofits.

Protecting yourself from scams

Fortunately, there are some things you can do to protect yourself from scams, including those related to the coronavirus pandemic:

- Don't click on suspicious or unfamiliar links in emails, text messages, and instant messaging services.
- Don't answer a phone call if you don't recognize the phone number — instead, let it go to voicemail and check later to verify the caller.
- Never download email attachments unless you can verify that the sender is legitimate.
- Keep device and security software up-to-date, maintain strong passwords, and use multi-factor authentication.
- Never share personal or financial information via email, text message, or over the phone.
- If you see a scam related to the coronavirus, be sure to report it to the FTC at ftc.gov/complaint.

[1] Internal Revenue Service, IR-2020-64, April 2, 2020
