Scammers are out there taking advantage of fears surrounding the Coronavirus. Please be aware of some of these scams and follow the tips below:

Treatment

Scammers are setting up websites to sell bogus cures, vaccines, and advice on treatments, and are using fake emails, texts, and social media posts to take your money and get your personal information. There are currently no vaccines, pills, potions, lotions, lozenges, other prescription or over-the-counter products available to treat or cure COVID-19.

Supply

Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.

Provider

Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.

Charity

Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.

Imposter

Scammers are posing as the Federal Deposit Insurance Corporation (FDIC) or the Federal Trade Commission (FTC), using the FDIC or the FTC name and logo, and may even include the real names of FDIC or FTC employees. These imposter scams are sent in a variety of ways; emails, phone calls (including robo calls), letters, text messages, faxes, and social media designed to;

- trick recipients into downloading malware, or providing personal identifying and financial information
- an offer to help victims of current or previous frauds with investigations or recovering losses
- ask for payment upfront before services can be provided
- threaten a lawsuit or arrest for an unpaid debt
- official looking forms for filing insurance claims, paying taxes on prize winnings, check endorsements, bankruptcy claimant verification forms, stock confirmations, and investment purchases
- receive a cashier's check with instructions to deposit the check and send some portion of the funds back via wire transfer service

Phishing

As with Imposter scams, scammers are posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails, designed to trick recipients into downloading malware, or providing personal identifying and financial information.

Apps

Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.

Investment

Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

Tips

- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Don't send money through any of these channels.
- Be wary of phone calls from someone claiming to be "family/friend" in distress and asking for money. Scammers spoof caller IDs and have the ability to clone a person's voice. You should hang up and call the family member or friend back to verify they were actually speaking with the family member or friend.
- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if there is a medical breakthrough, you won't hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Check the websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."
- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the general public this way.
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.
- Make sure the anti-malware and anti-virus software on your computer is operating and up to date.
- Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
- Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.
- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving. Remember, an organization may not be legitimate even if it uses words like "CDC" or "government" in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.
- Be cautious of "investment opportunities" tied to COVID-19, especially those based on claims that a small company's products or services can help stop the virus. If you decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website.
- For the most up-to-date information on the Coronavirus, visit the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) websites.