Surge in COVID-19 Scams

Fraudsters and scam artists have always looked for new ways to prey on consumers. Many are now using their tactics to take advantage of consumers' heightened financial and health concerns over the coronavirus pandemic. Federal, state, and local law enforcement have issued warnings on the surge in coronavirus scams and offer advice on how consumers can help protect themselves.

Here are some of the more prevalent coronavirus scams that consumers need to watch out for, along with some tips for protecting yourself from becoming the victim of a scam.

Fraudulent Treatments, Vaccinations, and Home Test Kits

The Federal Trade Commission (FTC) issued warnings about scam artists attempting to sell fraudulent products that claim to treat, prevent, or diagnose COVID-19. The FDA has warned consumers to be wary of companies selling products that are not authorized or approved by the FDA. You can visit fda.gov for more information.

Phishing Scams

Scammers have been using phishing scams related to the coronavirus pandemic to obtain personal and financial information. Phishing scams usually involve unsolicited phone calls, letters, 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. And remember that government organizations, such as the Social Security Administration and the Internal Revenue Service, will never initiate contact with you to ask for personal and financial information, such as your Social Security number. In addition, be on the lookout for nongovernment websites with domain names that include the words "coronavirus" or "COVID-19," as they are likely to be malicious.

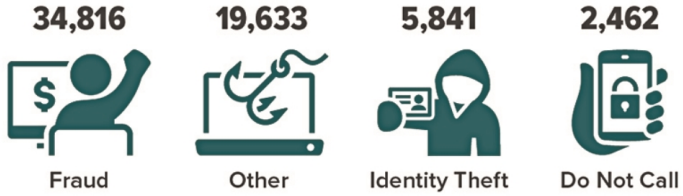
Coronavirus-Related Charity Scams

During the coronavirus pandemic, many charitable organizations have been established to help those affected by COVID-19. Unfortunately, scammers sometimes try to pose as legitimate charitable organizations in order to solicit donations from unsuspecting donors. Watch out for charities with names that are similar to more familiar or nationally known organizations such as the American Red Cross.

Before donating to a charity, make sure it is legitimate. 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.

FTC COVID-19 Complaints

Over 60,000 complaints related to COVID-19 were reported to the Federal Trade Commission during the period between January 1 and June 3, 2020, with a total fraud loss of $45.32 million.



Source: Federal Trade Commission, 2020

Protecting Yourself from Scams

Here are some steps you can take to help protect yourself from becoming the victim of a scam, including a scam related to the coronavirus pandemic:

- Don't click on suspicious or unfamiliar links in emails, text messages, social media feeds and instant messaging services.
- Don't answer a phone call if you don't recognize the phone number — 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 whenever possible.
- Never share personal or financial information via email, text message, or over the phone.

If you receive a fraudulent email, text or phone call, report it to the appropriate government agency such as the Federal Trade Commission or Internal Revenue Service and your local police department.