Avoiding Fraudulent Activity and Scams
We go to great lengths to protect your information. Below are tips to help you.

**Phishing** - Phishing is the criminal act of trying to get your information – usernames, passwords, social security numbers, and bank account or credit card account details – by pretending to be an entity you trust. Phishing e-mails often direct you to a website that looks real, but is fake, and may be infected with malware.

**Other Scams** - You may be the victim of a scam if someone claiming to be from the Census Bureau asks you for certain information. **The Census Bureau never asks for:**

- Your full Social Security number
- Money or donations
- Anything on behalf of a political party
- Your full bank or credit card account numbers
- Your mother’s maiden name

**What you can do** - Should you suspect fraudulent activity, please do the following:

- **If you get mail:**
  - Check that the return address is Jeffersonville, Indiana
  - If you continue to question the authenticity of the letter or form call the Regional Office for your state to verify the household survey. (See below)
○ **If someone calls your household** to complete a survey:
  - Call the National Processing Center to verify the caller is a Census Bureau employee.
    - 1-800-523-3205   Jeffersonville, IN
    - 1-800-642-0469   Tucson, AZ
    - **1-800-923-8282**   Customer Service Center

○ **If someone visits your residence** to complete a survey:
  - Check first for a valid U.S. Census Bureau ID badge
  - If you are still unsure then call the Regional Office for your state to verify you are in a legitimate survey and the visitor is a Census Bureau employee.

  **Fernando E. Armstrong, Regional Director**
  **Philadelphia Regional Office**
  100 South Independence Mall West - Suite 410
  Philadelphia, PA 19106-2320
  **(215) 717-1800 or 1-800-262-4236**
  FAX: (215) 717-0755
  TDD: (215) 717-0894
  E-mail: Philadelphia.Regional.Office@census.gov

○ **if you get an e-mail** and think it is bogus (fake):
  - Do not reply, do not click on any links, and do not open any attachments
  - Forward the e-mail or website URL to the Census Bureau at ois.fraud.reporting@census.gov
  - Delete the message. We will investigate and notify you of the findings.

    Reporting Suspected Fraud

If you suspect fraud, call **800-923-8282** to speak with a local Census Bureau representative. If it is determined that the visitor who came to your door does not work for the Census Bureau, contact your local police department.

Scammers are taking advantage of fears surrounding the Coronavirus.

Avoid Coronavirus Scams

Here are some tips to help you keep the scammers at bay:

- Don’t click on links from sources you don’t know. They could download viruses onto your computer or device.

- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying they have information about the virus. For the most up-to-date information about the Coronavirus, visit the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).

- Ignore online offers for vaccinations. There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores.

- Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don’t let anyone rush you into making a donation. If someone wants donations in cash, by gift card, or by wiring money, don’t do it.

What the FTC is Doing

The FTC and FDA have jointly issued warning letters to seven sellers of unapproved and misbranded products, claiming they can treat or prevent the Coronavirus. The companies’ products include teas, essential oils, and colloidal silver.

The FTC says the companies have no evidence to back up their claims — as required by law.

The FDA says there are no approved vaccines, drugs or investigational products currently available to treat or prevent the virus.
Checks from the Government  
March 18, 2020  
by Jennifer Leach Associate Director, Division of Consumer and Business Education, FTC

*** As the Coronavirus takes a growing toll on people’s pocketbooks, there are reports that the government will soon be sending money by check or direct deposit to each of us. The details are still being worked out, but there are a few really important things to know, no matter what this looks like.

1. The government will not ask you to pay anything up front to get this money. No fees. No charges. No nothing.

2. The government will not call to ask for your Social Security number, bank account, or credit card number. Anyone who does is a scammer.

3. These reports of checks aren’t yet a reality. Anyone who tells you they can get you the money now is a scammer.

*** Look, normally we’d wait to know what the payment plan looks like before we put out a message like this. But these aren’t normal times. And we predict that the scammers are gearing up to take advantage of this.

So, remember: no matter what this payment winds up being, only scammers will ask you to pay to get it.

If you spot one of these scams, please tell the Federal Trade Commission at: www.ftc.gov/complaint. We’re doing our best to stop these scammers in their tracks, and your report will help.

ftc.gov/coronavirus

Protect yourself from fraud  
medicare.gov/fraud

Scammers may use COVID-19 as an opportunity to steal your identity and commit Medicare fraud. In some cases, they might tell you they’ll send you a Coronavirus test, masks, or other items in exchange for your Medicare number or personal information. Be wary of unsolicited requests for your Medicare number or other personal information.

It's important to always guard your Medicare card like a credit card and check your Medicare claims summary forms for errors. Only give your Medicare number to participating Medicare pharmacists, primary and specialty care doctors or people you trust to work with Medicare on your behalf. Remember, Medicare will never call you to ask for or check your Medicare number.
Robocalls and stimulus check scams: two forms of fraud expected to increase due to coronavirus.

When news captures the public’s attention – think major hurricanes, terrorist attacks, and economic slowdowns – scammers come out of the woodwork to take advantage of legitimate fears and concerns. With coronavirus dominating the news globally, there is an unprecedented opportunity for criminals to use the public’s fears about the virus and the resulting economic downturn to defraud consumers. Two types of scams that are increasing due to coronavirus: robocalls and stimulus check scams.

Coronavirus-related robocalls

Robocalls are, at the very least, a major annoyance for most consumers. However, as the coronavirus has upended daily life, robocall operators have quickly shifted to blasting out spam phone calls offering all manner of coronavirus-related products and services. YouMail, a cloud-based telecommunications provider that tracks robocall volumes, estimates that at least one million robocalls per day are inundating Americans’ cell phones. Fraudulent robocallers are offering air duct sanitation services, work-from-home opportunities, cut-rate health insurance, and immune-system boosting nutritional supplements. Other robocalls have reportedly offered free insulin kits to diabetics, along with free coronavirus testing kits.

Our advice to consumers is simple:

1. If you receive a call from a number you don’t recognize, the safest course of action is simply to ignore the call.
2. If you answer a call and suspect it’s a robocall, simply hang up. Don’t press any of the numbers the message tells you to.
3. Never give any personal information, such as financial account number, Social Security number, full name, or mailing address to someone who contacts you via an unsolicited phone call or text message.
4. Do not click on any links sent to you via text message from someone you don’t know. They could lead you to malware or phishing websites.
5. If you’re being inundated by robocalls, your cellular provider may offer services that will increase the likelihood that the calls will be blocked.

Stimulus check scams

Last week, President Trump signed the biggest stimulus bill in U.S. history into law. Most American adults will receive a stimulus of $1,200 or more in the coming weeks thanks to
the legislation. Crooks are already using these promised payments as a way to defraud consumers. **Scams that have been reported involve crooks promising to expedite payment in exchange for a fee, impersonating a government official, and requesting sensitive personal information in order to process a check.** Inaccurate social media posts have also circulated suggesting that consumers need to fill out the 2020 Census before they can receive a stimulus check.

Consumers can protect themselves from these scams by learning to spot these red flags:

- The stimulus checks will be deposited automatically by direct deposit into consumers’ bank accounts for the vast majority of citizens who filed their taxes last year. Consumers without a bank account on record with the IRS will receive a paper check, but it may take several weeks longer to arrive than those who have bank accounts.
- Anyone who emails, texts, messages, or calls you claiming to be able to expedite your stimulus check is a scammer.
- Anyone who contacts you requesting sensitive information like PayPal account details, bank account information, or credit card numbers is trying to scam you.
- Your answers to the Census, and whether you’ve completed it, have no impact on your eligibility for a stimulus check.

These are just the tip of the iceberg when it comes to coronavirus-related scams. If you’ve been on the receiving end of a coronavirus-related phone call, email, or text message that you think is a scam, we want to hear from you! By filing a complaint at Fraud.org via our secure online complaint form you can help law enforcement bring scammers to justice. We share complaints with our network of nearly 200 law enforcement and consumer protection agency partners who can and do put fraudsters behind bars. **Scams can also be reported by phone to the FTC: 1-877-382-4357.**

---

You may already be taking steps to protect your health during the COVID-19 emergency. Be sure to also protect your identity from scammers by guarding your Medicare Number.

It's easy to get distracted and let your guard down during these uncertain times. **Scammers may try to steal your Medicare Number. They might lie about sending you Coronavirus vaccines, tests, masks, or other items in exchange for your Medicare Number or personal information.**

Protect yourself from scams:

- Only share your Medicare Number with your primary and specialty care doctors, participating Medicare pharmacist, hospital, health insurer, or other trusted healthcare provider.
- Check your Medicare claims summary forms for errors.

**To report Medicare fraud: 1-800-MEDICARE (1-800-633-4227)**
MORE CORONAVIRUS SCAMS

WEDNESDAY, APRIL 01, 2020

Robocalls and stimulus check scams: two forms of fraud expected to increase due to coronavirus.

When news captures the public’s attention – think major hurricanes, terrorist attacks, and economic slowdowns – scammers come out of the woodwork to take advantage of legitimate fears and concerns. With coronavirus dominating the news globally, there is an unprecedented opportunity for criminals to use the public’s fears about the virus and the resulting economic downturn to defraud consumers. Two types of scams that are increasing due to coronavirus: robocalls and stimulus check scams.

Coronavirus-related robocalls

Robocalls are, at the very least, a major annoyance for most consumers. However, as the coronavirus has upended daily life, robocall operators have quickly shifted to blasting out spam phone calls offering all manner of coronavirus-related products and services. YouMail, a cloud-based telecommunications provider that tracks robocall volumes, estimates that at least one million robocalls per day are inundating Americans’ cell phones. Fraudulent robocallers are offering air duct sanitation services, work-from-home opportunities, cut-rate health insurance, and immune-system boosting nutritional supplements. Other robocalls have reportedly offered free insulin kits to diabetics, along with free coronavirus testing kits.

Our advice to consumers is simple:

1. If you receive a call from a number you don’t recognize, the safest course of action is simply to ignore the call.
2. If you answer a call and suspect it’s a robocall, simply hang up. Don’t press any of the numbers the message tells you to.
3. Never give any personal information, such as financial account number, Social Security number, full name, or mailing address to someone who contacts you via an unsolicited phone call or text message.
4. Do not click on any links sent to you via text message from someone you don’t know. They could lead you to malware or phishing websites.
5. If you’re being inundated by robocalls, your cellular provider may offer services that will increase the likelihood that the calls will be blocked.

Stimulus check scams

Last week, President Trump signed the biggest stimulus bill in U.S. history into law. Most American adults will receive a stimulus of $1,200 or more in the coming weeks thanks to
March 31, 2020

[INFO] Information Only Alert – GIOC Reference #20-005-I
TLP Green

COVID-19 Stimulus Scams

Congress has recently passed a large COVID-19 relief and stimulus package. As with other aspects of the COVID-19 pandemic, fraudsters are exploiting the relief and stimulus to victimize the public. The U.S. Secret Service is observing a rise in stimulus relief fraud over the past several days and expect the fraud attempts to continue throughout the pandemic.

Criminal actors are using a variety of means to contact potential victims. In one instance, the criminal actors are using spoofed email addresses posing as U.S. Treasury officials requesting that the victim provide personal identifying information (PII), so that they can receive their share of the stimulus. A redacted example of an attack email is below:

From: U.S Treasury
Sent: [redacted] March 2, 2020
To: Recipients
Subject: COVID-19 Funds Release Update

New information is being released by The U.S. Treasury About The global funds release Programme, initiated by the world health organization (W.H.O) and empowered by The World bank Organisation.

Your are among the first Email ID batch list to receive payment $450,000.00 on this exercise, the purpose for these funds is to give relief to the global citizens of the world, due to corona virus pandemic which is the reason the world bank decided to carry out this exercise of empowerment to humanity globally.

You are assigned to a Senior supervisor Agent who will handle your filing and also monitor the processing of your funds release. He will also be responsible to give our office report about your empowerment funds usage.

We plan to create a world where everyone becomes financially independent, stable and individual accountability. You are to reconfirm your details below for immediate payment filing.

Full Name:
Address:
City / Country:
Profession:
Phone Number:
Gender:
Birth Date:
Identification

Sincerely
U.S Treasury Headquarters.
Treasury Building 1500 Pennsylvania Avenue,
NW Washington, D.C.,
United States Of America.

Other than via email, criminal actors are contacting potential victims via SMS/text, robocalls, and other messaging platforms. Through texts, criminal actors are sending links which directs individuals to a website, which then prompts the potential victim to enter PII and other sensitive information, such as bank account numbers, email addresses, and passwords. See below for an example of an attack SMS sent to a potential victim.

[INFO] - Indicates informational or educational content.
The attack above contained the victim’s real name, giving the text an appearance of legitimacy. Official stimulus/relief information regarding COVID-19 will never be sent via text/SMS or on any other messaging platforms.

Foreign partners are also seeing an uptick in COVID-19 stimulus relief fraud. The U.S. Secret Service anticipates instances of similar fraud affecting U.S. citizens in the coming weeks. The method is the same—a potential victim will receive a text message directing them to a link. Once they reach the link, they are prompted to enter a variety of PII data. See below for another example of these SMS/Smishing attacks received by our foreign partners.
Sunday, 22 March 2020

URGENT has issued a payment of 458 GBP to all residents as part of its promise to battle COVID 19. TAP here https://-covid-19.webredirect.org/ to apply

Enter Your Post Code To Apply for COVID-19 Relieve

NHS COVID-19 Relieve system.

The U.S. Secret Service stresses that individuals seeking information about the stimulus/relief program to contact the specific government agency via its website for guidance. Individuals should follow protocols published by those government websites. During this time, it is stressed that the public maintain an increased vigilance when providing any PII or other privileged and protected information.

Western Pennsylvania COVID19 Task Force

1-888-219-9372

Usapaw.covid19@usdoj.gov

pricegouging@attorneygeneral.gov

[INFO] - Indicates informational or educational content.
Fraudulent COVID-19 Emails with Malicious Attachments

During the coronavirus outbreak, many companies and organizations have sent emails containing COVID-19 updates to their customers to make them aware of their current response and status. As these types of emails have now become increasingly frequent, criminals have started to use this familiarity to their advantage. The USSS is aware of fraudulent emails, framed as a corporate COVID-19 response, which contain malicious attachments and are targeting individual consumers and corporations alike.

In the attempted attacks we are aware of, the malicious attachment would allow the attackers to remotely install malware on the infected system to potentially harvest credentials, install keyloggers, or lock down the system with ransomware. The impact of these type of attacks may not be immediately felt by the victim but may result in a BEC or other fraud in the future. The email attachment is frequently a Microsoft Office or WordPad file type, as so far, the attacks have utilized a now patched exploit of Microsoft Office. However, it is always possible that different variations exist, or the attack vectors will evolve. Corporations should be aware they are being targeted, with the attackers potentially posing as a vendor, member of the supply chain, or other familiar entities that would not seem out of place.

Dear Customers,

In the current environment of uncertainty, we at [REDACTED] are doing our utmost to care for your supply chain and serve you and your business as planned.


In the meantime, please remember to stay safe and look after yourself and your loved ones.

Regards,

The U.S. Secret Service has also received information regarding individuals receiving emails disguised as coming from a hospital that inform the recipient they may have come in contact with an individual who tested positive for COVID-19. The email instructs the recipient to download an attached Excel file, complete a form, and bring it to the nearest emergency clinic to be tested. As in the previous example, once the attachment is downloaded, the malware has been activated and the attackers may be able to:

- Steal log-in credentials for sites you have visited
- Look for open shares on the network and view all documents and folders
- Receive your IP address
- Discover and steal cryptocurrency wallet information

/RJ/

[INFO] - Indicates informational or educational content.
Another variation of this attack is an email purportedly from the U.S. Department of Health and Human Services. The email is targeting potential supplier companies by requesting they provide any medical protective equipment from an included product list with the attachment containing malware:

Dear supplier,
Due to the wild spread of COVID-19 all over the United States, the U.S. Department of Health & Human Services is in urgent demand of face mask and forehead thermometers for its citizens. I will like if your company can supply us with the attached products list.
Awaiting your urgent reply.

In most instances referenced above, the email signature blocks used the identity of a legitimate employee. Keep in mind that typically, legitimate COVID-19 response emails have a message only in the body of the email and do not contain attachments.

Western Pennsylvania COVID19 Task Force
1-888-219-9372
Usapaw.covid19@usdoj.gov
pricegouging@attorneygeneral.gov

/RJ/

[INFO] - Indicates informational or educational content.
the legislation. Crooks are already using these promised payments as a way to defraud consumers. **Scams that have been reported involve crooks promising to expedite payment in exchange for a fee, impersonating a government official, and requesting sensitive personal information in order to process a check.** Inaccurate social media posts have also circulated suggesting that consumers need to fill out the 2020 Census before they can receive a stimulus check.

Consumers can protect themselves from these scams by learning to spot these red flags:

- The stimulus checks will be deposited automatically by direct deposit into consumers’ bank accounts for the vast majority of citizens who filed their taxes last year. Consumers without a bank account on record with the IRS will receive a paper check, but it may take several weeks longer to arrive than those who have bank accounts.
- Anyone who emails, texts, messages, or calls you claiming to be able to expedite your stimulus check is a scammer.
- Anyone who contacts you requesting sensitive information like PayPal account details, bank account information, or credit card numbers is trying to scam you.
- Your answers to the Census, and whether you’ve completed it, have no impact on your eligibility for a stimulus check.

These are just the tip of the iceberg when it comes to coronavirus-related scams. If you’ve been on the receiving end of a coronavirus-related phone call, email, or text message that you think is a scam, we want to hear from you! By filing a complaint at Fraud.org via our secure online complaint form you can help law enforcement bring scammers to justice. We share complaints with our network of nearly 200 law enforcement and consumer protection agency partners who can and do put fraudsters behind bars. **Scams can also be reported by phone to the FTC: 1-877-382-4357.**

---

You may already be taking steps to protect your health during the COVID-19 emergency. Be sure to also protect your identity from scammers by guarding your Medicare Number.

It's easy to get distracted and let your guard down during these uncertain times. **Scammers may try to steal your Medicare Number. They might lie about sending you Coronavirus vaccines, tests, masks, or other items in exchange for your Medicare Number or personal information.**

Protect yourself from scams:

- Only share your Medicare Number with your primary and specialty care doctors, participating Medicare pharmacist, hospital, health insurer, or other trusted healthcare provider.
- Check your Medicare claims summary forms for errors.

**To report Medicare fraud: 1-800-MEDICARE (1-800-633-4227)**