



Avoid scams related to economic payments, COVID-19

Date: May 21, 2020 Joint Alert


Contact: newsroom@ci.irs.gov 

Overview

In March, Congress passed — and the President signed — the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a \$2 trillion economic relief package intended to support American businesses and individuals economically burdened by the coronavirus pandemic. A provision of the law includes sending economic impact payments to eligible Americans.

The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of the Treasury, the Internal Revenue Service (IRS), and the United States Secret Service (USSS) urge all Americans to be on the lookout for criminal fraud related to these economic impact payments—particularly fraud using coronavirus lures to steal personal and financial information, as well as the economic impact payments themselves—and for adversaries seeking to disrupt payment efforts.

For more information about economic impact payments, see the IRS [Economic Impact Payment Information Center](#), which includes answers to taxpayer questions about eligibility, payment amounts, what to expect, and when to expect it. See the IRS's article, [Do not let scammers get your COVID-19 Economic Impact Payment](#), for additional guidance.

To report an IRS-related coronavirus scam, visit the [Impersonation Scam Reporting](#)  webpage.

Call? Text? Email? Social Media?

The IRS will not call, text, email, or contact you on social media asking for personal or bank account information—even related to the economic impact payments.

Be suspicious of email with attachments or links claiming to have special information about economic impact payments or refunds.


See [Do not let scammers get your COVID-19 economic impact payment](#).


Technical Details

What are the threats?


COVID-related scams — The U.S. Government continues to encounter instances of criminals using stimulus-themed emails and text messages to trick individuals into providing personally identifiable information and bank account details. We recommend financial institutions to remind their customers about the importance of practices sound personal cybersecurity, to remain vigilant to illicit account use and creation, and to report potential crimes to either federal, state, or local law enforcement officials. See the following resources for more information:

- [CISA](#) 
- [FTC](#) 
- [FinCEN](#) 

To report a CARES Act fraud or other financial crime, contact your [local Secret Service field office](#) . Defrauding of government and financial institutions — We expect, at a minimum, criminals to use CARES Act-related and/or -themed emails or websites to trick financial institutions and their customers into providing criminals with personal or banking information or access to computer networks. Themes for these scams might include economic stimulus, personal checks, loan and grant programs, or other subjects relevant to the CARES Act. These CARES Act-related cybercriminal attempts could support a wide range of follow-on activities that would be harmful to the rollout of the CARES Act.

On the most dangerous end of the spectrum, criminals and adversaries may pursue activities that go beyond stealing information or funds and seek to disrupt the operations of the organizations responsible for implementing the CARES Act, including through the use of ransomware to extort money from victims, steal personal information, or interrupt the flow of CARES Act funds. We recommend federal, state, local, and tribal agencies and financial institutions initiate a comprehensive security review of critical systems, especially those involved with banking, payments, and loan processing. Further, please visit [CISA's Ransomware](#)  page for information about this specific threat.



Countering these threats

- The U.S. Government and international partners have increased their distribution of threat intelligence and best practices to industry and local governments to achieve the immediate effect of disrupting and deterring this criminal activity. See the CISA and the United Kingdom's National Cyber Security Centre (NCSC) alerts on [COVID-19 Exploited by Malicious Cyber Actors](#)  and [APT Groups Target Healthcare and Essential Services](#)  for more information.
- The USSS is focusing its investigative operations on ensuring that those who seek to exploit this pandemic are brought to justice, and that the proceeds of their criminal activity are recovered; these investigations will include actions over the near term, but also in the coming months and years to hold criminals accountable and recover assets. See the Secret Service's [alert on phishing](#)  during COVID-19, and [guide to identifying a legitimate stimulus check](#) .

Mitigations

Understand how the IRS communicates electronically with taxpayers

- The IRS does not initiate contact with taxpayers by email, text messages, or social media channels to request personal or financial information.

- This includes requests for personal identification numbers (PINs), passwords, or similar access information for credit cards, banks, or other financial accounts.
- The official website for the IRS is www.irs.gov though some stimulus recipients may also need to use this IRS-run site, [Free File Fillable Forms](#) . Beware of similar domain names and mismatched SSL certificates. Navigate to the [official site](#) to avoid mistyping the domain name.
- To prepare for—or respond to—a criminal incident review the [Preparing For A Cyber Incident](#) .



Take action to avoid becoming a victim

If you believe you might have revealed sensitive information about your organization or access credentials, report it to the appropriate contacts within the organization, including network administrators. They can be alerted for any suspicious or unusual activity.

Watch for any unexplainable charges to your financial accounts. If you believe your accounts may be compromised, contact your financial institution immediately and close those accounts.

If you believe you might have revealed sensitive account information, immediately change the passwords to those accounts. If you used the same password for multiple accounts, make sure to change the password for each account and do not use that password in the future.



Report suspicious phishing communications

- Email: If you read an email claiming to be from the IRS, do not reply or click on attachments and/or links. Forward the email as-is to phishing@irs.gov , and delete the original email.
- Website: If you find a website that claims to be the IRS and suspect it is fraudulent, send the URL of the suspicious site to phishing@irs.gov  with subject line, "Suspicious website."
- Text Message: If you receive a suspicious text message that claims to be from the IRS, do not reply or click on attachments and/or links. Forward the text as-is to the IRS at [202-552-1226](tel:202-552-1226) (standard text rates apply), and then delete the original message (if you clicked on links in SMS and entered confidential information, visit the IRS's [identity protection](#) page).

If you are a victim of any of the above scams involving IRS impersonation, please report to phishing@irs.gov, and [file a report](#)  with the Treasury Inspector General for Tax Administration, the [Federal Trade Commission](#),  and the police. To report a crime, contact your [local Secret Service field office](#) .

Additional Resources

For more information on phishing, other suspicious IRS-related communications, including phone or fax scams, or additional guidance released by Treasury/IRS, CISA, and the Secret Service visit:

- [Avoiding Social Engineering and Phishing Attacks](#) 
- [Recognizing and Avoiding Email Scams](#) 
- [Phishing and Other Schemes Using the IRS Name](#)
- [IRS Phone Scam Intensifies During Filing Season](#)
- [Report Phishing and Online Scams](#)

Additional Reporting Activity

To report an intrusion and request technical assistance, contact CISA at cisaservicedesk@cisa.dhs.gov or [888-282-0870](tel:888-282-0870), or FBI through a [local field office](#) or the Internet Crime Complaint Center (IC3) at www.ic3.gov. For law enforcement assistance, please contact your [local U.S. Secret Service Field Office](#). If you are the victim of tax-related identity theft, please follow the guidance at the [Taxpayer Guidance to Identity Theft](#).

Page Last Reviewed or Updated: 15-Mar-2021