

# Stimulus Check Fraud – Avoid Being Scammed

According to the Federal Trade Commission (FTC), there have been more than \$200 million in stimulus check losses due to scams and fraud.

## How is this happening?

Fraudsters are versatile and inventive. They're scamming people via several avenues.

Fraudsters send emails with links that look legit but will infect your computer with malware if you click on it. The malware captures personal info that enables the fraudster to steal your money.

An easy way to see if there is something fishy with a link, is to hover your mouse over it and look to see if the address that shows up makes sense. Fraudulent links usually show weird unrelated addresses when you hover over them. The best practice is not to click on any links coming from an email you haven't interacted with before.

Fraudsters will also call and impersonate the IRS. **BEWARE.** The IRS won't call you. They will send you a letter. Typically that letter is a certified. Many times the fraudster is calling to claim they need paid some sort of fee in order to process your stimulus check. This is false. The fee is just a way to get you to give them your credit or debit card information.

There have also been reports of fake stimulus checks. Keep in mind, if you've received your stimulus money via electronic deposit to your account, you'll not receive a paper check. If a person deposits this fake check, they will then get a call from a fake IRS agent asking for the money to be returned due to an error. A few days after the money is returned per the fake IRS agent instructions... the fake check will have failed to clear your account and the account holder is on the hook for the amount of the check.

Fraudsters are always working on ways to steal your money.

## Ways to protect yourself

1. Don't open unsolicited emails, especially from unfamiliar people or companies.
2. Don't click on links from unfamiliar emails, especially emails claiming to be from the IRS. The IRS does not send unsolicited emails.
3. Beware of checks that are way more than expected. The government has many checks and balances to make sure they don't over pay. If it seems too good to be true, call the IRS directly to verify.
4. Don't be threatened. Fraudsters are pushy and sometimes downright rude and abusive. Don't tolerate it. Just hang up.
5. NEVER give out sensitive personal or account information. The IRS does not need your debit or credit card number for anything associated with a stimulus payment.
6. If you don't recognize the email address, delete the message. If you don't recognize the phone number, don't answer. Most fraudsters won't take the time to leave a message. If they do leave a voicemail don't return the call. If you are compelled to return a call based on the message. Look up the phone number on your own via Google or a phone book and call a published number.
7. If in doubt, CALL the CREDIT UNION before taking any action. We're trained to spot fraud and can help you decipher whether you are being targeted as a victim.
8. Trust your internal alarm (a.k.a. intuition, gut reaction). Typically, it is not wrong.

We are here to help safeguard your money! If you think something seems odd with a situation, call us. It's easier to avoid fraud than it is to recoup money lost due to a scam.

There are several ways to reach us...  
515-243-8735 (2nd Ave location)  
515-282-3606 (SE 14th St location)  
askus@journeycu.org  
info@journeycu.org  
LIVE CHAT with us as [www.journeycu.org](http://www.journeycu.org)

*We are working hard for hard working people.*