Is that stimulus payment message a scam?

Fake emails, texts and phone calls about these payments have risen 6,000% in recent weeks. Here are clues that fraudsters are trying to steal your money.

? A message about your payment arrives as an email, text, social media post or phone call.

✕ **The IRS only communicates by mail.**

? The "IRS" claims you must first make a payment in order to get a stimulus payment.

✕ **Fraudsters claiming to be with the IRS often insist you make a payment using iTunes gift cards, money orders, debit cards, or a wire transfer.**

? The "IRS" demands financial information before it can process your payment.

✕ **The IRS has your financial information. It's fraudsters who want it.**

? An email refers to your "stimulus check" or "coronavirus check".

✕ **The IRS will only refer to the payment as an "economic impact payment."**

? An email about your stimulus payment, ordering personal protective equipment or virus testing directs you to a professional-looking website with the word "coronavirus" in the web address.

✕ **Tens of thousands of fake websites that include the words "coronavirus" or "COVID" have been created in recent weeks.**

? The email urgently requests a donation and provides a link to the Red Cross.

✕ **Emails are often designed by fraudsters to collect personal information, not to help a charitable organization. To make a donation, visit the Red Cross website directly.**

? Whoops: the "IRS" says it mistakenly paid you too much and demands you return money.

✕ **The IRS doesn't do that. Fraudsters do.**

? A phone call or email promises to speed the deposit of your stimulus payment if you provide personal information.

✕ **The only way to check on the status of your payment or provide information is to visit the IRS "Get My Payment" website.**

? Unless you send money immediately, an email threatens to go public with embarrassing information about you and displays personal information like one of your passwords to prove they're serious.

✕ **The password was stolen in an earlier data breach. Change the password wherever it's used and ignore the email.**

? A fake email or text has a link to "opt out" of future messages.

✕ **These links only prove scammers that they've reached a working address.**

DANAHER
INFORMATION SECURITY
THINK PROTECT SECURE TOGETHER