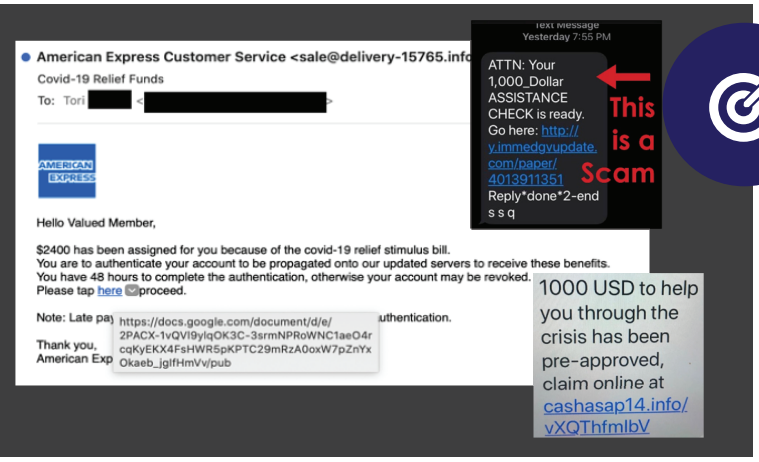
FRAUD UPDATES:

BEWARE OF STIMULUS CHECK-RELATED SCAMS



As U.S. citizens begin to receive notifications regarding Government-issued stimulus checks—formally known as economic impact payments—malicious actors are conducting online scams to steal money or sensitive information from victims using phishing emails, text messages, and social media messages, among other tactics. While there are no indications that the Department of the Navy family is being specifically targeted, please be vigilant and do not reply to these messages.

Actors often impersonate financial institutions, the Internal Revenue Service, charities, and other businesses to request victims verify personal or financial information in order to receive a stimulus check or request a fee for quicker processing of the payment. Actors may also attempt to deliver malware to victims via a malicious link.

In other versions of stimulus check-related scams, actors mail fake checks to victims and request them to verify information online or via phone in order to cash the check. Other fraudulent checks appear to offer the victims more than what they are owed and include requests the difference back in online money transfers, gift cards, or cash.

RED FLAGS

• Request for personal and/or financial information in order to receive stimulus checks is delivered via email, phone, social media, or text message. A legitimate bank or agency would never request personal and/or financial information using these tactics.

• Promises for a faster payment if the victim clicks a link, provides sensitive information, or pays a fee.

• Message includes grammar, spelling errors, or typos within the content of emails or messages
• Message is delivered from an unknown sender or the sender appears to be an official from the IRS, White House, or other agency that does not typically reach out for sensitive information.

• Message includes the term "stimulus check" or "stimulus payment. Official government documents will use the official term "economic impact payment."

If you have been targeted with this scam, call NCIS or use NCIS Tips via www.ncis.navy.mil or downloading our app via iTunes or GooglePlay.

1-800-386-8762