UNCLASSIFIED

CHICAGO POLICE DEPARTMENT CPIC CRIME PREVENTION & INFORMATION CENTER FEDERAL STATE AND LOCAL JOINT VENTURE

Chicago Police Department
Crime Prevention & Information Center
Private Sector Situational Awareness Bulletin

(U) SITUATIONAL AWARENESS - FRAUD SURROUNDING COVID-19

Please be aware that fraudsters are attempting schemes in order to obtain money or sensitive information from individuals receiving the United States Treasury Economic Impact Program (EIP) payments. It should be known that neither the IRS nor any other federal agency will call, text, e-mail or contact an individual on social media asking for personal or bank account information - even related to the economic impact payments.

Recently, there has been an increase in phishing schemes utilizing e-mails, letters, texts and links. These contacts will often come in the form of unsolicited e-mail and/or websites that pose as legitimate sites in an effort to lure unsuspecting victims to provide personal and financial information. Scammers will often use website names similar to valid ones, for example IRSGOV, IRS GOV, or using extra letters and/or spaces in lieu of IRS.GOV.

A recent example of fraud involves phishing e-mails coming from "customer_service@FreeFillableForms.com" which directs you to a link that contains "economic impact payment" and uses a company name similar to the Free File Alliance partner you are transferred to while using the IRS tool for Non-Filers. DO NOT click on the link - this is a scam. Other phishing schemes are using keywords such as "Corona Virus", "COVID-19", and "Stimulus" in varying ways."

Other historical fraud methods have been modified for COVID-19 fraud. These include:
- **Testing scams:** An unsolicited offer of testing that asks for health insurance information. Scammers use such offers to fraudulently bill insurance or federal health care programs for COVID-19 tests. If those claims are rejected, the victim could be responsible for the bill, according to the U.S. Health and Human Services website. The scammer could gather information for medical identity theft, a form of identity fraud.
- **Demands to pay for a friend's or relative's care:** Scammers pose as medical professionals treating a friend or relative and demand immediate payment. Do not provide any information or payment.
- **Fake charities:** Fraudsters use the images and stories of real people and exploit generosity to steal. The Federal Communications Commission offers tips for verifying whether a charity is legit. • Grandchild or other "person in need": An email, message or phone call says a family member is suffering from COVID-19 and needs help buying groceries, paying for care or getting food delivered.
- **App scams:** Criminals are creating apps that say they'll help track the spread of COVID19. Instead, they insert malware that can harvest your personal information.
- **Social Security threats:** Criminals have seized the opportunity with the closure of Social Security offices. They contact recipients, saying they must provide personal information or pay to maintain benefits. The Consumer Financial Protection agency warns that any communication saying that benefits will be suspended or reduced due to COVID-19 is a scam.
- **Employment opportunities:** The advice of not paying to get a job has never been more relevant. With many people desperate for work, scammers offer bogus job openings.

The FBI's Internet Crime Complaint Center has received more than 3,600 complaints about websites peddling fake vaccines or cures, soliciting donations for fake charities, falsely representing themselves as public health organizations or exploiting concern over the virus to trick users into downloading malware.

Scams and frauds can be reported to the following agencies:
Federal Trade Commission https://www.ftccomplaintassistant.gov/#crnt
National Center for Disaster Fraud Hotline at 1-866-720-5721 or e-mail at disaster@leo.gov
Cyber scams can be submitted through the FBI's website https://www.ic3.gov
Suspicious e-mails can also be reported to the IRS at phishing@irs.gov

Tracked by HSEC – 8.2, 8.3 and 8.8.