UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

CID Warns of Increase in COVID-19 Related Fraud, Scams

QUANTICO, Va. (April 6, 2020) – The U.S. Army Criminal Investigation Command continues its commitment to ensuring the health and safety of the Army family and recommends being suspicious of anyone offering unsolicited advice on prevention, protection or recovery during the COVID-19 pandemic.

Opportunistic scammers continue to find creative ways to obtain and use someone's personal and financial information. From fake stimulus checks to Medicare fraud, cybercriminals will undertake extreme measures to separate individuals from their money.

"With the passing of the nearly $2 trillion dollar stimulus bill, cybercriminals around the world are already looking at ways to exploit it," said Edward Labarge, director, of CID's Major Cybercrime Unit. "During tax season, we see a massive uptick in the amount of tax-related fraud schemes. With the new stimulus bill, we night see a massive uptick in the amount of stimulus and debt relief scams circulating on the internet."

CID officials remind the Army community that stimulus checks will come directly from the Internal Revenue Service (IRS) and service members should deal only with the IRS. Reliable COVID-19 stimulus information is available on the IRS website.

Labarge encourages people to, "ignore all phone calls, emails, and text messages of anyone asking you for personal information to receive stimulus aid." The U.S. Government will not ask you for your private information. If you believe you've been a victim of a scam, contact your nearest CID office.

-MORE-

Known types of scams:

Medical Supply/ Treatment Scams: Currently, there are no FDA approved home test kits. Ignore social media or other online offers for home test kits or vaccinations to treat or prevent COVID-19. Visit www.fda.gov to learn more. Be cautious when ordering Personal Protective Equipment (PPE) such as masks, gloves, hand sanitizer or other medical or health equipment that is in high demand. Scammers will pitch products creating fake stores online and utilizing social media to lure purchases of these items to steal your money and not deliver items promised. Scammers will also offer to sell fake cures, vaccines or COVID-19 test kits.

Imposter Scams: Don't respond to texts, emails or phone calls requesting personal, banking or health information. Scammers are also contacting people by phone and email, pretending to be doctors, hospitals that have treated a friend or relative for COVID-19, or claiming before treatment can be given demand payment. These calls typically try to create panic and rush decision-making. Pressure tactics include threats of repercussions if not paid immediately. Legitimate agencies will not resort to these tactics.

Charity scams: During challenging times, scammers know people want to help others less fortunate and will exploit this generosity soliciting donations for individuals, groups, or areas affected by COVID-19.

Stimulus Check Fraud: With the recent approval of stimulus checks, scammers will be especially creative to obtain personal and banking information through the use of imposter schemes, robocalls, emails or texts requesting information to "ensure" payment is received on time. The stimulus check will be a one-time direct payment delivered by the IRS to individual taxpayers mainly through direct deposit based on information in the previous year's tax return. There is no need to sign up and no one from the IRS will call or email you to confirm personal or bank information.

In addition, the Criminal Investigation Command's Major Cybercrime Unit continues to warn the Army community of ongoing COVID-19 themed phishing attacks impersonating organizations with the end goal of stealing information and delivering malware.

"Cybercriminals are innovative and will take advantage of current browsing trends to conduct social engineering attacks," said Labarge. "We have already seen this with malware infected COVID-19 maps and phishing emails related to the pandemic."

Labarge said the Major Cybercrime Unit continues to "aggressively pursue cybercriminals both domestic and abroad who target our Soldier's and their families in their online campaigns."

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil.

-30-