UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

CID Encourages Vigilance to Prevent COVID-19 Cyber Scams

QUANTICO, Va. (March 13, 2020) – During this time of heightened awareness and protection against potential health risks associated with COVID-19, there is also an increased risk in scam methods used by cybercriminals.

The U.S. Army Criminal Investigation Command warns the Army community that some phishing campaigns prey on would-be victims' fear, while others capitalize on the opportunity created by hot topics in the news cycle. The COVID-19 Pandemic presents cybercriminals with a way to combine both into a dangerous one-two punch.

Most recently, the Johns Hopkins University COVID-19 interactive map has been hacked by cybercriminals. The hackers are selling copies of the interactive map as a malware tool used to steal passwords and user data.

A significant number of additional coronavirus-related domains have been registered. CID officials warn users to not open attachments or links in emails coming from such domains.

Below is a list of websites that have recently shown signs of malicious behavior detected by anti-virus software:
coronavirusstatus.space
coronavirus-map.com
blogcoronacl.canalcero.digital
coronavirus.zone
coronavirus-realtime.com
coronavirus.app
bgvfr.coronavirusaware.xyz
coronavirusaware.xyz

-MORE-

Army CID Special Agents are reminding people to be alert and suspicious and take extra steps to verify information before agreeing to anything putting that could put one's personal or financial information at risk.

According to CID officials, individuals should be suspicious of anyone who approaches or initiates contact regarding coronavirus; anyone not known, or with whom conversation was not initiated, who offers advice on prevention, protection or recovery – especially if they ask for money. Cybercriminals may use a variety of approaches. Below is a potential list of approaches that could be used:

- Someone claims to represent the health department who emails you or comes to your door and tells you of the risks of COVID-19 and offers you vaccination or other testing. The health department will not do this. This is a dangerous scam. If this happens, call your local police department immediately.
- Someone claiming to be from your bank or an investment firm who you do not already have a relationship with, who offers investment alternatives to protect you from economic and market uncertainties.
- Someone who threatens you with repercussions (arrest, prosecution, confinement) if you don't pay a fee.
- Someone claiming to be from a hospital where a loved one is being treated for the virus but is in urgent need of money before lifesaving treatments can be rendered.
- Someone claiming to be your friend who is stuck in a foreign country and can't get home unless a "virus prevention" or other outrageous sounding fee is paid.
- Unsolicited emails offering expert advice or information. They could contain malware or the links in the email could take you to a site with malware.
- Someone asking for any personally identifiable information, bank account or financial information, or information about family members.
- Someone claiming to be from computer support who tells you your computer is infected with corona virus and offers to repair it. (Your computer cannot be infected by corona virus.)

CID officials also remind individuals to remain vigilant and take precautions against cyber scams. They also recommended to always use trusted sources; avoid clicking on links in unsolicited emails, IMs, or texts; avoid opening attachments in unsolicited emails; do not reveal personal or financial information in email, IMs, or texts; and verify a charity's authenticity before making donations.

Additional information on COVID-19 – progression, transmission, symptoms, treatment – may be found at reputable websites for the Centers for Disease Control and Prevention, World Health Organization, The U.S. Department of Health and Human Services, U.S. Food and Drug Administration, the U.S. Government's Corona Virus website, your state, county or city health department, your local hospital, your primary care physician, the local free clinic or wherever you receive medical services.

-30-

For more information about computer security, other computer-related scams and to review previous cyber crime 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.