Cybercrime Prevention Flyer

CPF 0004-20-CID361-9H **11 March 2020**

The Corona Virus, Cybercriminals and You

This Cybercrime Prevention Flyer is about the methods by which cybercriminals might capitalize on the uncertainty and fear brought about by reports of the corona virus – COVID-19. This flyer is not a comprehensive list – there are too many methods to list and cybercriminals are a very creative and adaptive bunch.

Think of this flyer as a strong reminder to be suspicious. To go the extra step to verify before you agree to anything that puts you personally or financially at risk. Or before giving any personally identifying information to anyone you do not know.

Be suspicious of anyone who approaches you or initiates contact regarding corona virus. Be suspicious of anyone you don't know or with whom you did not initiate a conversation who offers you advice on prevention, protection or recovery – especially if they ask for money.

Cybercriminals could use any and many different approaches. Look out for these kinds of approaches:

- 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.)

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

Cybercrime Prevention Flyer

This Cybercrime Prevention Flyer is not related to any medical diagnosis or infection prevention.

If you need information on the corona virus – progression, transmission, symptoms, treatment – check reputable websites like 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's, county's or city's health department, your local hospital, your primary care physician, the local free clinic. Or wherever you receive medical services.

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF