UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

CID Cautions Teleworkers to Adhere to IT Best Practices

QUANTICO, Va. (March 23, 2020) – As the Army community continues to encourage teleworking, the U.S. Army Criminal Investigation Command reminds users about cyber adversaries and the importance of keeping all information on the network safe.

As telework increases across the Army, network users play an important role in protecting the Department of Defense Information Network. CID encourages users to follow department-issued guidance and best practices as well as those developed by DoD. This information will help ensure users maintain secure use of common capabilities and continue to operate effectively during telework status.

CID officials also remind the Army community that your government furnished equipment (GFE) is for official government use only and is to be used only by authorized users. It is important to remind family members the computer is for your work only and not to be used for other purposes. Users are encouraged to utilize good practices such as locking and removing your CAC and maintaining the physical security of their GFE.

Additional important reminders for government teleworkers:

- The use of Government Furnished Equipment is ALWAYS the preferred method for connecting to DoD Resources
- Adhere to your organization-specific Telework User Guidance
- Use your organization's official connection services while conducting official business (e.g., VPN, MobiKEY, Skype for Business, and VidyoDesktop etc.) and log off from connection at the end of work day or during idle times when you are not directly interacting with network resources.
- While connected to the NIPRNet, use of streaming video/audio and internet access is not authorized except for official business

-MORE-

- Study and follow the Acceptable Use Policy for government systems
- Use your organization's approved communication and collaboration methods for official business
- Work offline whenever possible

In addition, the Criminal Investigation Command's Major Cybercrime Unit continues to warn the Army community of ongoing Coronavirus-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 Edward Labarge, Director, Major Cybercrime Unit, USACIDC. "We have already seen this with malware infected COVID-19 maps and phishing emails related to the pandemic."

Labarge recommends always inspecting the URL and ensuring you know where the link will take you, because criminals are disguising themselves in an effort to steal money and/or sensitive information.

"When conducting research on COVID-19 or any other topic, you want to ensure you use good cybersecurity best practices," he said. "This includes keeping your browser, operating system, and antivirus software up to date. Additionally, you should never click on an unknown link. You can check the link by hovering your mouse over the URL to see where it leads."

Some Trusted Sources available for use:

* DAF COVID-19 Webpage: https://www.af.mil/News/Coronavirus-Disease-2019/

* Centers for Disease Control and Prevention (CDC) COVID-19: https://www.cdc.gov/coronavirus/2019-ncov/index.html

* USAF COVID-19 Information Page: https://www.af.mil/News/Coronavirus-Disease-2019/

* World Health Organization: https://www.who.int/

Please continue to exercise proper cyber hygiene while utilizing VPN and government computers as well as personal devices.

-30-

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