Cybercrime Prevention Flyer

CPF 0007-2020-CID361-9H **08 April 2020**

Video Conferencing Services & Your Safety

As the COVID-19 pandemic has brought about mandated social distancing, to stay in touch with loved ones, collaborate with coworkers, and even attend medical appointments, video-teleconferencing (VTC) has become more and more popular. But, like always, if it's popular with the public, it's also a popular exploit of criminals.

Cybercriminals are able to exploit VTC software—whether it's a paid service or free—to obtain sensitive information or even eavesdrop on conference calls and virtual meetings. To gain access, cybercriminals might employ phishing, spoofed links or mobile applications that appear to come from legitimate VTC vendors.

In addition to cybercriminals, some VTC software companies may not have your best interest in mind. One well-known VTC company is currently being sued for allegedly selling user data to third parties including a popular social media company. According to the lawsuit, the VTC company, after a user logged on, provided the third party with customer information, including details of the device used.

As always, you should apply cyber best practices and weigh associated risks to ensure privacy and protect critical information. Consider the following steps:

- Verify the link to the meeting you attend is legitimate.
- Make sure to download the VTC software from the correct website.
- Verify the meeting ID and dial-in information is legitimate.
- Do not make meetings public.
- Do not share a link to a teleconference in an unrestricted, publicly available social media post. Provide the link directly to specific people.
- Avoid remote desktop sharing.

Below is a list of approved collaboration software for Army personnel to use for official telework purposes; however, please contact your system administrator for additional guidance on approved VTC software.

- DISA Global Video Service (GVS)
- Defense Collaboration Services (DCS)
- Skype for Business
- Intelink
- milSuite
- DoD Commercial Virtual Remote (CVR) Environment

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

DISTRIBUTION:
This document is authorized for the widest release without restriction.

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