THE FACTS: TIPS FOR SECURE TELEWORKING

As more and more Army employees are teleworking nowadays, away from traditional government places of duty, good all-around network security and telework practices become even more vital.

Here are some good guidelines and tips:

-- Always use your organization's approved communication and collaboration methods for official business

-- Always use organization-approved file sharing services and capabilities to share files

-- Don't use government-furnished equipment for personal or non-essential activities such as social networking, audio and video streaming or online shopping

-- Remember that government-furnished equipment is for official government use only and should not be used only by authorized users

-- Do not add unauthorized hardware or software to government-owned computers

-- Study and follow the Acceptable Use Policy for government systems

-- Don't leave video collaboration tools such as video, voice or email connected or running when they're not actively in use

-- Reboot computers prior to establishing a VPN connection

-- Keep systems updated with the latest updates and security patches

ABOUT US: U.S. Army Cyber Command integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. **As of 16 July 2018**

.

-- Configure home Wi-Fi according to best practices for maximum security

-- Create a strong, unique password and network name for your Wi-Fi

-- When given the option, use added security authentication factors in addition to passwords

-- Remember to log off, remove Common Access Cards and lock machines when they are not in active use

-- Be careful to maintain good physical security of government-furnished equipment

-- Work offline whenever possible

Follow ARCYBER on
(click the images to visit our pages)

Cyber

.