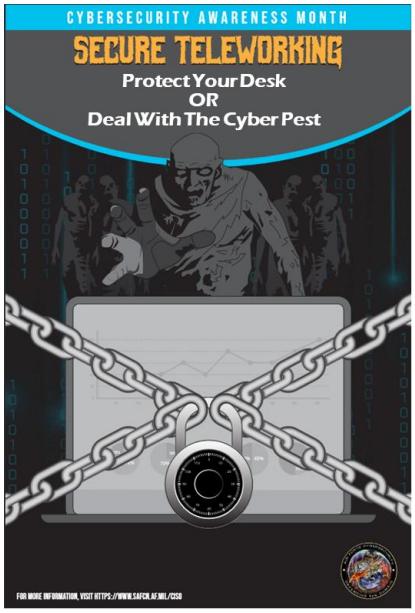
Air Mobility Command Cybersecurity Awareness Month Newsletter

18 October 2021 Vol II Issue III

CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart

Week 3: Secure Teleworking & 2-Factor Authentication



For more information contact your Wing CyberSecurity Office or e-mail the HQ AMC Cybersecurity Office at AMC.Cybersecurity@us.af.mil

SECURE TELEWORKING

The Federal Government is a leader in the use of innovative workplace arrangements like telework. In June 2014, President Obama issued a Presidential Memorandum titled **Enhancing Workplace Flexibilities and Work-Life Programs** to help attract, empower and retain a talented and productive workforce in the 21st century. Visit the following site for more telework information: https://www.telework.gov/federal-community/telework-managers/telework-basics/

Knowing your organization's policies and procedures and completing mandatory security training can help ensure you are compliant with teleworking requirements. You should never connect your government laptop to a public Wi-Fi network. Adversaries can intercept transmissions from your laptop and steal your information.

BEST TELEWORKING PRACTICE

Do's:

- Only use agency-approved video conferencing collaboration tools and methods to share files
- Whenever possible, only use laptops and smartphones owned, managed, and protected by your agency
- Store work-related content on Government Furnished Equipment (GFE) and agency-approved cloud services
- Only connect GFE to a network you are in complete control of (e.g., home network)

Don'ts:

- Don't forward work emails to a personal account
- Don't store work-related content on personally-owned equipment (e.g., laptops and cell phones)
- Don't print work-related content at home (unless explicitly approved by our agency)
- Don't use your GFE or government desktop session for nonwork-related activities such as social networking, audio and video streaming, or personal shopping

Use 2-Factor Authentication When Available

2-factor authentication, sometimes referred to as multi-factor authentication, is a security process in which a user provides two different authentication components to verify themselves. This offers stronger security against an unauthorized third party from accessing a user's personal or financial data than a single password.

Who Uses Two-Factor?

CSAM Virtual Events and other resources are available at: https://www.safcn.af.mil/Organizations/CISO-Homepage/Cybersecurity-Awareness-Month-CSAM/CSAM-2021/