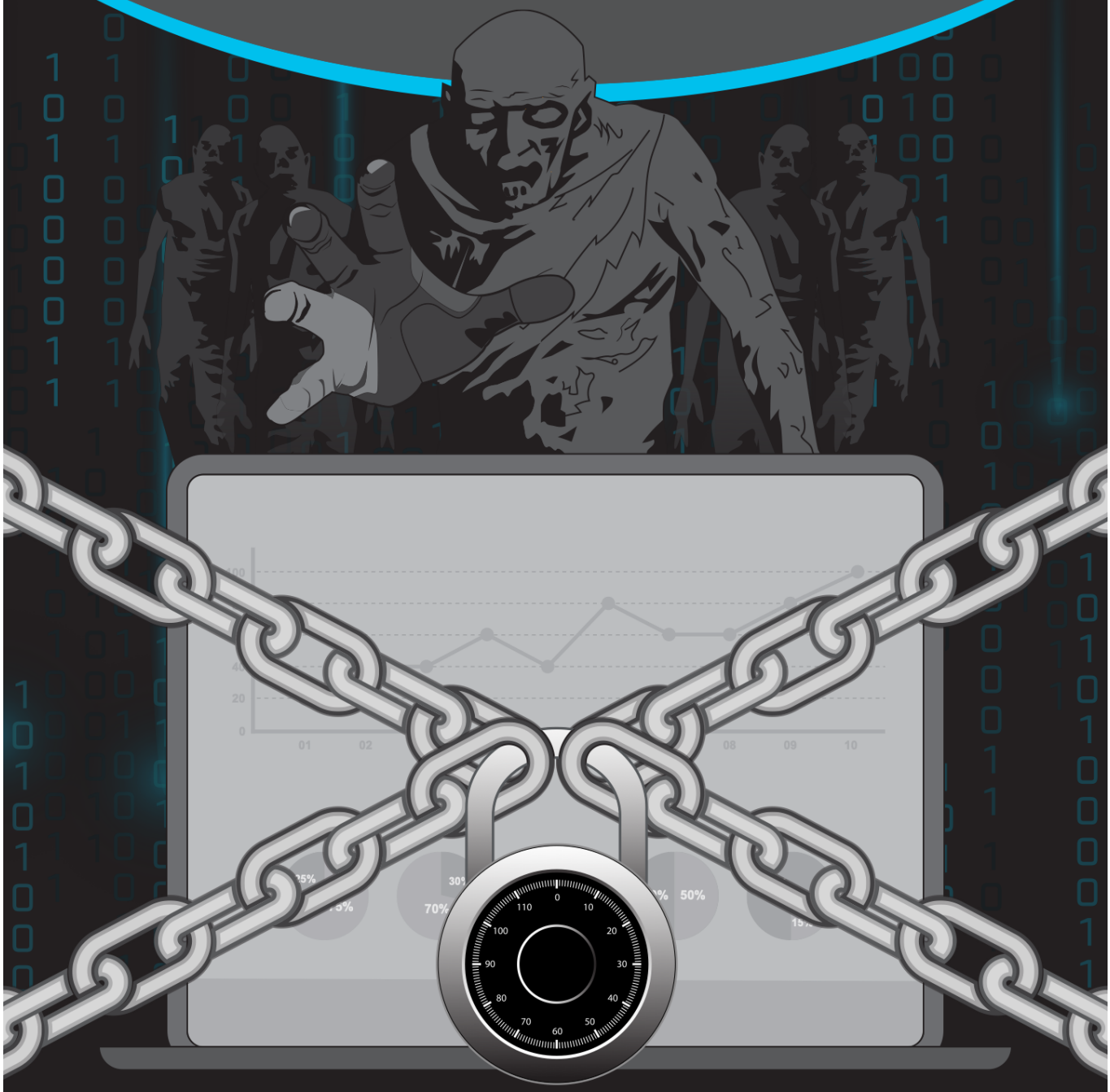
CYBERSECURITY AWARENESS MONTH

SECURE TELEWORKING

"PROTECT YOUR DESK OR DEAL WITH THE CYBER PEST"



FOR MORE INFORMATION, VISIT HTTPS://WWW.SAFCN.AF.MIL/CISO

Secure Teleworking

Teleworking Defined:

A work arrangement in which an employee performs their responsibilities and duties from an approved worksite (e.g. home) other than the original official workspace. Most DAF personnel telework regularly, which is anticipated to continue well into the future as DAF policy is revised to encourage the flexibility provided by extensive teleworking.

However, teleworking introduces new risks to DAF information and resources. The use of official webmail on personal machines presents an opportunity for transferring information to systems and areas not intended to process government information. Always follow DAF teleworking guidance, available on the AF Portal. Security of your home office is now an essential aspect of protecting DAF information, systems, and resources.

#BeCyberSmart

Helpful Ways To Secure Teleworking:

- Avoid using public Wi-Fi, and make sure your home Wi-Fi has a strong password. Be sure networking devices have software patches applied when made available.
- Only store work-related files and content on your government computer/device.
- Update your government computer/device firewall, antivirus software, and other applications when updates are available.
- Never connect your government computer to your home printer or other devices with data storage capabilities
- If using government webmail on a personal device, update the device's operating system and applications when needed.

#CyberForMe

Lock your computers and remove your CAC card when taking breaks to prevent unauthorized access to sensitive information. Report suspicious activities you notice on your assigned computer to your help desk or Comm Focal Point ASAP.

Free Anti-virus for DoD employees:

McAfee Antivirus software

https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/antivirus-home-use