CYBERSECURITY AWARENESS MONTH

WEEK 1

CYBERSECURITY AWARENESS MONTH

WHAT YOU SHARE
MAY COME BACK TO HAUNT YOU

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

WEEK 2

CYBERSECURITY AWARENESS MONTH

PHISHING AND RANSOMWARE
"DON'T TAKE THE BAIT"

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

WEEK 3

CYBERSECURITY AWARENESS MONTH

SECURE TELEWORKING
"PROTECT YOUR DESK OR
DEAL WITH THE CYBER PEST"

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

WEEK 4

CYBERSECURITY AWARENESS MONTH

BE MINDFUL OF
ALL CONNECTED DEVICES
"PROTECT YOUR CONNECT!"

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

DON'T LET ZOMBIES OWN YOUR CYBERSECURITY!
#BECYBERSMART #CYBERFORME

AIR FORCE CYBERSECURITY ★ DEFENDING THE DOMAIN ★

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

Viruses, Trojans, Spyware, Ransomware, and Hackers are few of the things that could harm your devices, networks, or steal your information. There are several precautions to avoid becoming a victim of (or an easy target for) cyber criminals.

Knowledge is Key

Staying informed and practicing good cyber hygiene is the easiest way to avoid becoming a victim of (or an easy target for) cyber criminals. Here are few ways you can protect your devices and your personal information:

- Set all social media accounts to hide your personal information from other users.
- Enable login (or activity) alerts, and security questions (2FA/MFA) for your accounts.
- Install and update security software on your devices.
- Update all devices software, and remove outdates Apps from devices & home networks.
- Run SCANS on any downloaded files or programs before opening.
- Turn OFF your Bluetooth, Wi-Fi, and GPS system when not in use.
- Do NOT open phishing e-mails.
- Do NOT connect to unknown / unsecure Wi-Fi.
- Do NOT share personal information online.
- Do NOT download pirated software, movies, music, or files. [can attract legal sanction]
- Verify links (and URLs) before clicking on them.
- Be very mindful of all the Internet of Things (IoTs) devices you are connected to.

Strong Passwords

Having strong unique passwords can help protect your accounts, devices, and networks. It is recommended to use a password manager (or vault) to store your passwords. A password manager maintains all of your usernames and passwords, and usually has the capability to generate unique passwords. Some password managers uses biometrics login, to protect your stored login information. Here are few characteristics and recommendations to creating a strong password:

- Password length – eight (8) or more characters
- Use numbers, uppercase and lowercase letters, special characters, spaces
- Use random and/or complex password
- Do NOT recycle or reuse passwords
- Do NOT use personal information (birthdays, SSN, family/pet names)
- Example of a strong password –
  Cy8er_$ecur!Ty

Two-Factor or Multi-Factor Authentication (2FA/MFA)

Multi-Factor Authentication (MFA) does add another layer of protection to your accounts. Factor authentication uses different form factors to verify your identity. Several different authenticators that you can utilize includes biometrics, tokens, or applications (Apps).

You can download authentication applications from the Google Play store or Apple store. The authentication application (App) links your account with your device. The Authentication App provides you with a one-time code to access your account. Here are few different types of authenticators that you can utilize:

Google or Microsoft Authenticator

- Can be used on Android, iOS, or PC
- Must have device to generate code, and you must manually enter the code

LastPass Authenticator

- Used as browser extension or application
- Uses One-tap system to login, verifies your authentication via prompt on your device

Hardware: Physical security key fob, USB-drive, or Electronic-card that generates login code

Teleworking (keep secured)

Lock your computers and remove your CAC card when taking breaks, to prevent unauthorized access to sensitive information. Report suspicious actives you notice on your assigned computer ASAP.

Anti-virus or Anti-malware Software

The easiest ways to protect your system and devices is by installing a well-rounded security suite. You will benefit from using software that scans for viruses, malware, blocks harmful files, and identifies potential phishing e-mails and fake websites.

Free Anti-virus for DoD employees

- McAfee Antivirus software (free)
- For personal device
- For active DOD employees and authorized government contractors
- CAC reader required to access link below

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

Protect Your Information and Devices

Provided below are few security suites you can compare for your personal devices. Included are the features of each security suites that will aid you in making an informed decision. Some of the security suites do offer a free version, with lesser features.

MalwareBytes (Security + VPN)

- Prevents threats in Real-Time
- Crushes Ransomware
- Defends against harmful sites
- Cleans and removes malware

Bitdefender (Security + VPN)

- Optimizer that cleans unnecessary files
- Anti-Phishing protection from email scams
- Protect information with Privacy Firewall
- Browse anonymously with Unlimited VPN
- Prevent hackers from accessing your Microphone and Webcam

Norton 360 Premium I (Security + VPN + *etc.*)

- Anti-Spyware, Antivirus, Malware, and Ransomware Protection
- Secures VPN and Smart Firewall
- Dark web monitoring
- Password manager
- Cloud backup (100GB)
- Parental controls
- SafeCam (protects webcams)
- Online Threat Protection
- School Time (manage child's activities)

McAfee Ultimate (Security + VPN + *etc.*)

- Secure VPN (5 licenses)
- Antivirus and Malware protection
- Network security
- Password manager
- Safe web browsing
- Performance optimization
- McAfee Gamer Security
- Identity theft Insurance (protection)
- McAfee Shredder (delete sensitive files)

Cyber Helpful Hints

- Strong Password
- 2FA (MFA) for all accounts
- Antivirus and VPN on devices
- Lock your screens (setup auto-lock)
- Turn OFF Bluetooth, GPS (when not in use)
- Always scan all devices and files
- Update all devices/applications
- Mindful of IoT devices

Cybersecurity: Own It.

#BeCyberSmart

#CyberForMe