◊ Durable
  - Can only be used on sites that support FIDO or FIDO2F

◊ Thetis BLE Security Key
  - Very durable
  - Bluetooth capabilities

Knowledge is Key

What is another great and free way to protect your devices? Knowledge! Staying informed and practicing good cyber hygiene is the easiest way to ensure that you do not become a victim of or easy target for cyber criminals. Here are several ways you can protect your systems:

◊ Do not give out or post personal information online.
◊ Set social media accounts to hide your personal information from other users.
◊ Enable login or activity alerts and security questions for your accounts.
◊ Ensure you have security software installed on your devices.
◊ Do not connect to unknown or unsecure Wi-Fi.
◊ Shut off your Bluetooth, Wi-Fi, and GPS when you are not using them.
◊ Do not download pirated software, movies, music, or files.
◊ Run scans on any downloaded files or programs before opening.
◊ Be aware of phishing e-mails, and do not open e-mails from unknown senders.
◊ Verify links before clicking on them and URLs before going to them.

Wanda T. Jones-Heath
Chief Information Security Officer (CISO), DAF
Twitter: @SAF_DCIO
@SAF_CISO
https://www.safcn.af.mil/ciso/

Air Force Cybersecurity
To assure the effectiveness of Air Force's core missions by increasing the cybersecurity and resiliency of systems and information

PROTECTING INFORMATION AND DEVICES

Characteristics, Generators and Vaults

#BeCyberSmart

Protect Your Information and Devices

Viruses, Trojans, Spyware, Ransomware, and Hackers are just a few of the things that could harm your devices, your network, or steal your information. However, there are several precautions you can take to ensure that you do not become a victim of or easy target for cyber criminals.

Anti-virus or Anti-malware Software

One of the easiest ways to protect your system and devices is to install a well-rounded security suite. You will benefit from using software that scans for viruses and malware, blocks potentially harmful files and downloads, and assists in identifying potential phishing e-mails and fake websites. Here are a few of the more well-known security suites; their prices; and capabilities, so you can make a more informed decision about choosing protection for your devices—some of the software listed may also have a free version:

MalwareBytes

◊ Price - $70 – 1 device for 2 years
◊ Capabilities:
- Removes malware and spyware
- Real-time virus and malware protection 24/7
- Stops exploit/ransomware attacks
- Shields against malicious websites

Bitdefender

◊ Price - $40 – 5 devices for 1 year
◊ Capabilities:
- Real-time virus and malware threat detection
- Stops exploit/ransomware
- Secures VPN
- Parental controls
- Dedicated browser to protect against malicious websites

Norton 360

◊ Price - $40 – 5 devices for 1 year
◊ Capabilities:
- Real-time virus and malware threat protection
- Secures VPN
- Dark web monitoring
- Password manager
- Cloud backup
- Parental controls
- SafeCam (protects webcams)
- Performance optimization

McAfee

◊ Price - $45 – 10 devices for 1 year
- Real-time virus and malware protection
- Performance optimization
- Network security
- Password manager
- Safe web browsing
- Encryption storage
- Identity theft protection

Create Strong Passwords

Having strong passwords can help protect your accounts, devices, and networks. However, it can be difficult to create strong, unique passwords for every login and remember all of them as well. For this reason, it is recommended to use a password manager or vault. They can maintain all of your usernames and passwords, and most have the capability to generate new passwords. You will still need to create a password for your manager (if it doesn't use biometrics), and it will need to be strong since it will be protecting all of your login information. Here are a few characteristics and recommendations to keep in mind when creating a strong password:

◊ Use Spaces
◊ Do not recycle or reuse passwords
◊ Make it long
◊ Use letters and numbers
◊ Use uppercase and lowercase letters
◊ Use special characters
◊ Make it random
◊ Do not use personal information (birthdays, SSN, family/pet names)

Multifactor Authentication

Multifactor authentication can add another layer of protection to your accounts, and when paired with login or attempted login notifications, can ensure you have full awareness and control over your accounts. There are several different authenticators that you can utilize, including biometrics, tokens, or applications. Here are a few different types of authenticators that you can utilize:

Applications: You can download these from the Google Play store or Apple store. To use, simply enable authentication on your account, and scan the QR code to add the account to the application. This will link your device to the account and provide you with a code (which changes every few seconds) which will be used to log into the account.

◊ Google Authenticator
- Overall, one of the best authenticator apps
- Can be used on Android, iOS, or PC
- Must have device to generate code, and you must manually enter the code

◊ 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
- Browser extension or application
- Uses a one-tap system to log in that then verifies you are trying to log in by acknowledging a prompt on your device

◊ Hardware: You have a physical security key fob, USB, or card that you must connect to your device or use to generate a code to log into your accounts.

◊ Yubico Authenticator
- Very durable
- Uses a one-tap approach with a round button that, when pressed, generates your code
- Can be used as FIDO or 2FA
- Comes in USB-A and USB-C
- Titan Security Key