Air Mobility Command
National Cybersecurity Awareness Month
Newsletter

12 October 2020 Vol 1 Issue 2

Do Your Part.

#BeCyberSmart

October is National Cyber Cybersecurity Month

Week 2: Passwords & PINS

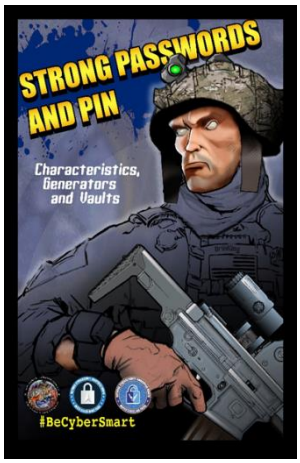
- What is a Password
- PINs for Home & Work
- Password Managers
- Password Passphrase

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

Most common, not recommended, password types (Google Survey, 2013):

- *Anniversary date*
- *Birthday*
- *Favorite holiday*
- *Birthplace*
- *Name of family member*
- *Pet's name*
- *The word "password"*
- *Sports team or item*

Passwords are a method to authenticate access/permission to an area or data. "Watchwords" were the earliest examples of passwords used in the Roman military. Passwords for military purposes evolved to include a counter-password to act as a confirmation. In the opening days of the 1944 Battle of Normandy, American Paratroopers used a device called a "cricket" in place of a password system as a temporary unique method of identification. One click given by the device was the call out and two clicks was for the reply. In 1961, MIT's Compatible Time-Sharing System was the first computer that used a password logon. This was one of the first inter-user messaging systems, that later evolved to today's email.



Personal Identification Number (PIN) for Home Computers: Windows 10 uses an option called "Hello PIN," working in conjunction with the hardware Trusted Platform Module (TPM), installed in PCs after 2009. The TPM generates and sends an encrypted user key to Microsoft authentication servers to validate the user. If an incorrect PIN is used, the user must validate their identity with a Microsoft representative before device access is restored. Typically, PINs are 4 to 8-digit numbers but for home PCs they can, and should, be just as complex as passwords. TPM can also be the gateway for biometric login methods, such as fingerprint, facial, or iris recognition, but the PIN is still your emergency backup.

PINs for Work Computers with a Common Access Card (CAC)/token is the current government authentication solution. While this method is not as complex as the Microsoft Hello PIN/TPM, the PIN/CAC is a two-factor authentication method that works great for government system since this requires physical possession of daily-validated CAC and knowledge of the associated PIN.

Password Managers for home use will store your credentials in a virtual locked vault accessed by a single master password or by two-factor authentication. Instead of reusing a single password for several accounts, like email and banking, you can use a password manager to have strong, unique passwords for each of your accounts without having to memorize them all.

Passwords that meet standards can be challenging—at least eight characters long containing upper and lower case letters, a number, a special character, and then, sometimes changing it every 2 months. One method is to create a passphrase you can recall like, "I absolutely like peanut butter and strawberry jam sandwiches at 1530." Using the first letter of each word, incorporating numbers and symbols and you get the strong password IaLp3&SjS@1530.

Lastly, avoid passwords that include favorite sports team player and jersey number, favorite car and/or license plate number, or anything else published in social media. Remember, BeCyberSmart.