



Department of Information Technology

Office of Information Security

LEARN HOW TO CREATE PASSWORDS

1. Do not use words found in any dictionary, spelled forward or backward.
2. Do not display passwords on screens or any other media at any time, and do not store passwords in clear-text (unencrypted) form.
3. Employ appropriate actions to prevent observers from viewing passwords.
4. Practice entering your password so that it can be entered quickly using several fingers.
5. Use your body to prevent the observer from seeing the keys being pressed as you enter your password.
6. Request that guests do not watch the password entry process.
7. Perform the password entry prior to demonstrating system use.
8. Change your password when it has been compromised, or when you suspect that it has been compromised.
9. Memorize your password. Do not write down or store passwords in batch files, automatic log-in scripts, software macros, terminal function keys, or any place where others might discover them.
10. Never use the built-in feature of **any** system to save your password or remember your password for you. If you do, your password may be saved/remembered in a clear and readable form that hackers can easily find.
11. Do not disclose or share your password with anyone.

To construct a strong password that is easy to remember, use the initial letters of a phrase (use both upper and lower case), and include a number or special character.

For example, if you like to go on vacation, you might take the letters from:

My Favorite Vacation Spot Is Cabo San Lucas Mexico

You would get: **Mfv\$1c\$LM**

- something that you can remember, but that would be hard for an attacker to guess.

By the Way – **DO NOT** use the **Mfv\$1c\$LM** example as your password.