What makes a password strong?

Cyber criminals use sophisticated tools that can rapidly decipher passwords. A strong password:

- Is at least eight characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four categories: uppercase letters, lowercase letters, numbers and symbols.

Avoid creating passwords that use:

- Dictionary words in any language.
- Words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters. Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty).
- Personal information. Your name, birthday, driver's license, passport number, or similar information.

Help yourself remember your strong passwords

- Switch letters with numbers(e=3; s=5; a=4; i/l=1; o=0)

- Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as, "My son's birthday is 12 December, 2004"
    - *Msbi12/Dec,4*
    - *Mi$un's Brthd8iz 12124*

- Relate your password to a favorite food, hobby, movie, song or book.
    - "I love to play badminton" could become *ILuv2PlayB@dm1nt()n.*
    - "Who you gonna call? Ghost Busters" could become *WyGC?G0B*
    - *c01in#l1ke5#ch33s3*

- Create 3 "levels' of passwords:
    - A easy one you use all the time for the "throw away" accounts (registering for random sites) that do not have confidential data (PD360, Atomic Learning)
    - A single secure one for most work accounts. When you change one, change the others too (Aeries, Windows, DataDirector)
    - One for each financial account that need to be highly secure

- Use a standard password and add a tag for the site
    - qfT99-email
    - qfT99-website
    - qfT99-aeries

- Save a password hint in your web browser's bookmarks or favorites list to indicate the starting letter and number of characters (*CAHSEE D------ C------)*