Password Tips

The more we use accounts like FaceBook, Instagram, emails, and so on, the more we have to be careful with the way we protect our accounts. This is where passwords have a very important role on security. Here are some tips to help you select good passwords and avoid bad ones:

1. When it comes to passwords, the longer the better for security reasons. Your new password must be 8 characters or longer and must be a mixture of letters, numbers and symbols. Follow this tips:
    1.1. If mixed case letters, numbers and symbols, use 8-11 characters.
    1.2. if mixed case letters and numbers, use 12-15 characters.
    1.3. If used only case letters, user 16-19 characters.
    1.4. 20+ characters need no restrictions.

2. It must not be a word that appears in the dictionary.
    2.1. Avoid adding prefixes or suffixes to any word. For example $money$ is not a secure password.

3. Also, avoid the following:
    3.1. Passwords based on a dictionary word spelled backward (sttesuhcassam).
    3.2. Passwords based on two dictionary words in a row (dogdog).
    3.3. Passwords based on the person's name.
    3.4. Passwords that are all white space.
    3.5. Passwords that contain control characters.
    3.6. Passwords that are all numbers.
    3.7. Passwords followed and/or preceded by 1 or 2 characters (9cheval, cheval9, 99cheval, cheval99, 99che val99 etc.)
    3.8. Passwords with several repeating characters (aaaaaaaa or aaaabbbb or abababab).
    3.9. Passwords that do not have more than 4 characters that differ from the previous character by one (1234abcd).
    3.10. Passwords with license plate patterns (daaaddd).
    3.11. Passwords with social security patterns (dddssdddd).
    3.12. Passwords with phone number patterns (dddsdddd or dddsdddsdddd).

Password Tips

So, how can I create more secure passwords?

4. Longer passwords are better passwords. The more characters a password cracking program has to crunch, the harder it is to guess.

5. Remove all the vowels from a short phrase in order to create a "word."

    Example: llctsrgry ("All cats are gray")

6. Use an acronym: choose the first or second letter of your favorite quotation.

    Example: itsotfitd ("It's the size of the fight in the dog")

7. Mix letters and non-letters in your passwords. (Non-letters include numbers and all punctuation characters on the keyboard.)

8. Transform a phrase by using numbers or punctuation.

    Examples: Idh82go (I'd hate to go), UR1drful (you are wonderful).

9. Avoid choosing a password that spells a word. But, if you must, then:

    9.1. Introduce "silent" characters into the word. Example: va7ni9lla

    9.2. Deliberately misspell the word or phrase. Example: choklutt

    9.3. Choose a word that is not composed of smaller words.

    9.4. Add random capitalization to your passwords. Capitalize any but the first letter.

    9.5. A random mix of alphabetical, numeric and symbolic characters.

        Example: eIeIoH!, o.U.Kid

    9.6. Long word and number combinations. For example, take four words, and put some numbers between them: stiff3open92research12closer

    9.7. An acronym for your favorite saying, or a song you like.

        Example: GykoR-66 (Get your kicks on Route 66) or L!isn! (Live! It's Saturday Night!).

    9.8. An easily pronounced nonsense word with some non-letters inside.

        Example: slaRoo@Bey or klobinga-dezmin.

10. Change your password at least once a year. Better yet, change your password every few months to shrink your exposure window. You can make three or four passwords if you like, then switch them throughout the year.

11. Don't use the same password on multiple accounts. When one site is compromised, hackers try to use those passwords to access accounts on other sites. Don't let one break-in give hackers access to all your accounts.

Taken and adapted from:

www.kb.mit.edu/confluence/display/istcontrib/Strong+Passwords & www.uit.stanford.edu/service/accounts/passwords