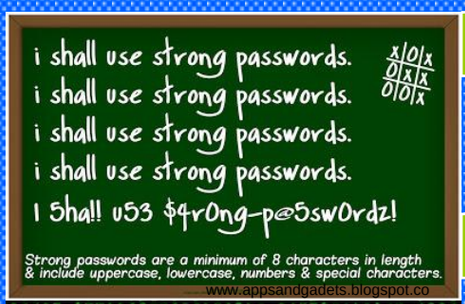
December 05, 2014 Release # 295

-- Begin Transmission --

How to choose secure passwords

Passwords are your protection against fraud and loss of confidential information, but few people choose passwords that are really secure.



✓Make your password as long as possible

The longer a password is, the harder it is to guess or to find by trying all possible combinations (i.e., a brute force attack). Passwords of 14 characters or more are vastly more difficult to crack.

✓Use different types of characters

Include numbers, punctuation marks, symbols, and uppercase and lowercase letters. On mobile devices that are not designed for easy special character input, consider using longer passwords with different characters.

✓Use passwords that are difficult to identify as you type them in

Make sure that you don't use repeated characters or keys close together on the keyboard.

✓Consider using a passphrase

A passphrase is a string of words, rather than a single word. Unlikely combinations of words can be hard to guess.

×Don't use dictionary words

Don't use words, names or place names that are usually found in dictionaries. Hackers can use a dictionary attack (i.e., trying all the words in the dictionary automatically) to crack these passwords.

×Don't use personal information

Other people are likely to know information such as your birthday, the name of your partner or child, or your phone number, and they might guess that you have used them as a password.

×Don't use your username

Don't use a password that is the same as your username or account number.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): Sophos Ltd. (2012). *Threatsaurus: The A-Z of computer and data security threats.* Boston, USA | Oxford, UK