Windows 7

Tips for creating strong passwords and passphrases

A password is a string of characters used to access information or a computer. Passphrases are typically longer than passwords, for added security, and contain multiple words that create a phrase. Passwords and passphrases help prevent unauthorized people from accessing files, programs, and other resources. When you create a password or passphrase, you should make it strong, which means it's difficult to guess or crack. It's a good idea to use strong passwords on all user accounts on your computer. If you're using a workplace network, your network administrator might require you to use a strong password.

Note

In wireless networking, a Wi-Fi Protected Access (WPA) security key supports the use of a passphrase. This passphrase is converted into a key that is used for encryption, which is not visible to you.

What makes a password or passphrase strong?

A strong password:	A strong passphrase:
• 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.	• Is 20 to 30 characters long. • Is a series of words that create a phrase. • Does not contain common phrases found in literature or music. • Does not contain words found in the dictionary. • Does not contain your user name, real name, or company name. • Is significantly different from previous passwords or passphrases.

Strong passwords and passphrases contain characters from each of the following four categories:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c

Character category	Examples
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

A password or passphrase might meet all the criteria above and still be weak. For example, *Hello2U!* meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. *H3ll0 2 U!* is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

Help yourself remember your strong password or passphrase by following these tips:

- 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*. Using that phrase as your guide, you might use *Msbi12/Dec,4* for your password.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, *My son's birthday is 12 December, 2004* could become *Mi$un's Brthd8iz 12124*, which would make a good passphrase.
- Relate your password or passphrase to a favorite hobby or sport. For example, *I love to play badminton* could become *ILuv2PlayB@dm1nt()n*.

If you feel you must write down your password or passphrase to remember it, make sure you don't label it as such, and keep it in a safe place.

Creating stronger passwords and passphrases using ASCII characters

You can also create passwords and passphrases that use extended ASCII characters. Using extended ASCII characters helps make your password or passphrase more secure by increasing the number of characters you can choose from to make it strong. Before using extended ASCII characters, make sure that passwords and passphrases containing them are compatible with the programs that are used by you or your workplace. Be especially cautious about using extended ASCII characters in passwords and passphrases if your workplace uses several different operating systems or versions of Windows.

You can find extended ASCII characters in Character Map. Some extended ASCII characters should not be used in passwords and passphrases. Do not use a character if a keystroke is not defined for it in the lower-right corner of the Character Map dialog box.

Windows passwords can be much longer than the eight characters recommended above. In fact, you can make a password up to 127 characters long. However, if you are on a network that also has computers

running Windows 95 or Windows 98, consider using a password that is no longer than 14 characters. If your password is longer than 14 characters, you might not be able to log on to your network from computers running those operating systems.