How to use ASCII characters to create strong passwords

When you create a password or passphrase, you should make it strong, meaning it is very difficult to guess or crack. You should use strong passwords with all user accounts on your computer.

Password is a string of characters used to access confidential information, networks, mobile devices or computers. Passphrases are often longer than passwords, to enhance security and contain many words that make up that passphrase.

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, meaning it is very difficult to guess or crack. You should use strong passwords with all user accounts on your computer. If you are using the network at work, your network administrator may require you to use strong passwords.

Note : In a wireless network, a protected Wi-Fi security key (WPA) supports the use of a passphrase. This passphrase is converted into a key, used for encryption, and you cannot see it.

How to use ASCII characters to create strong passwords

What makes a strong password or passphrase?

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 of the following 4 types:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
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	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

Passwords or passphrases can meet all of the above criteria and remain weak. For example, **Hello2U!,** Meets all the criteria for a strong password listed above, but is still weak, as it contains a complete word. **H3ll0 2 U!,** Is a more powerful alternative, because it replaces some letters in the complete word with numbers and includes spaces.

1. Notes when setting a password

Tips for remembering your strong password or passphrase

1. Create an acronym from an easy-to-remember piece of information. For example, choose a meaningful phrase for you, such as 'My son's birthday is 12 December, 2004' (my son's birthday is December 12, 2004). Use the initials of that phrase as your password. For example, you can use **Msbi12 / Dec, 4** as your password.

2. Replace numbers, symbols and misspellings for letters or words in that easy-to-remember phrase. For example, 'My son's birthday is 12 December, 2004' could become **Mi $ un's Brthd8iz 12124** , and that would

create a good passphrase.

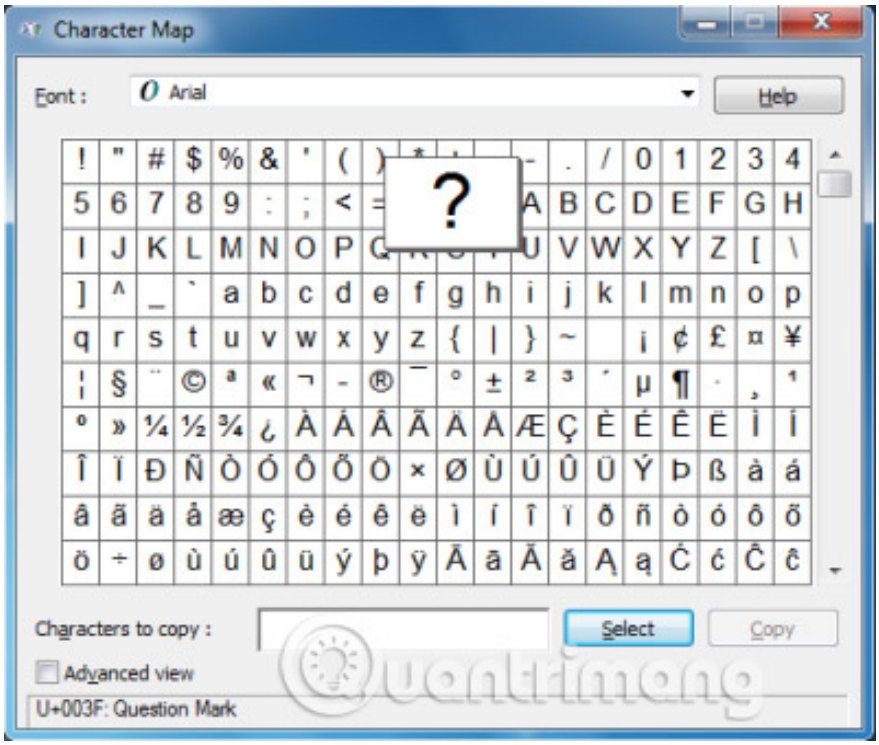
3. Link your password or passphrase to your favorite hobby or sport. For example, 'I love to play badminton' can become **ILuv2PlayB @ dm1nt () n.**

4. If you feel you have to write your password or passphrase to remember them, make sure you don't label the password and keep the password in a safe place.

Create stronger passwords and passphrases with ASCII characters

You can also create passwords and passphrases using extended ASCII characters. Using extended ASCII characters makes your password or passphrase safer, by increasing the number of characters you can choose, to make the password strong. Before using extended ASCII characters, make sure that the password and passphrase contain them, compatible with the programs used by you or your workplace. Be especially careful when using extended ASCII characters in passwords and passphrases, if your workplace uses multiple operating systems or different Windows versions.

You can find extended ASCII characters in Character Map. Some extended ASCII characters should not be used in passwords and passwords. Do not use characters, if a shortcut is not defined in the lower right corner of the Character Map dialog box.



Windows 7 or Vista passwords can be longer than 8 characters, as suggested above. In fact, you can create passwords up to 127 characters long. However, if you're on a network with a Windows 95 or Windows 98 computer, consider using a password that is no longer than 14 characters. If your password is longer than 14 characters, you may not be able to log into your network from computers running those operating systems.

See more:

1. ASCII encoding and Latin character table ISO 1252
2. How can Windows passwords be cracked?
3. Instructions for creating images in ASCII Art code style

You finished reading the article "**How to use ASCII characters to create strong passwords**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
