

PASSWORD.EXE

PASSWORD.EXE is a password maker that allows for the creation of a very complex password that can be retrieved and recreated without recourse to mental gymnastics or actually writing it down. This might help to minimize the use of easy-to-crack simple passwords that have been highlighted lately in the news. You only have to commit to memory ONE number that is no larger than 7-digits for ALL of your applications.

All you have to remember is:

- (1) The Application that uses the password
- (2) All the EXACT Characters NOT allowed (Illegal Characters)

An example of characters that MAY NOT be allowed are the following 17 characters: "*+,. /;<=>?[\\]~

- " (double quote)
- * (asterisk)
- + (plus sign)
- , (comma)
- . (period)
- / (forward slash)
- : (colon)
- ; (semicolon)
- < (less than)
- = (equals sign)
- > (greater than)
- ? (question mark)
- [(left bracket)
- \ (backslash)
-] (right bracket)
- | (vertical bar or pipe)
- ~ (tilde)

- (3) Whether or not to allow duplicate characters
- (4) The EXACT Key that was used (Up to a ± 7 -digit number with decimals allowed) (Memorize the Key!)
- (5) The EXACT Sub-Key to use with different applications
- (6) The Password Length

The list of illegal characters is not meant to be all inclusive and may include characters that are legal. You have to test each application that requires a password to see if you have generated a password that has illegal characters with your choice of the Key. Then, you can use the same Key by adding the illegal characters to the characters not allowed and try again. In other words, you do not have to change your chosen Key or Sub-Key.

With this information, a complex password can be created and will be the same for every running of the program. The length of the password is from 4 characters (PIN) up to 80 characters - depending upon the choices made. Note that the Key in (4) is NOT written down - it must be memorized. However, the information from (1), (2), (3) (5), and (6) can be safely recorded for reference so that the exact password can be regenerated on demand. The SAME memorized secret Key can be used with DIFFERENT Sub-Keys and will ALWAYS generate DIFFERENT Passwords for different applications.

An example of one application in a recorded text file list is as follows: (Assume my "MEMORIZED" Secret Key is: 12345.67 which is NOT recorded anywhere)

(1) MyOnlineBanking.com

(2) Illegal Character: "*+,./:;<=>?[\\]|~

(3) No Duplicates

(5) Sub-Key = 89

(6) Password Length = 15

Password Generated: **-BD@XpvoHFnU%r7**

If the Sub-Key **(5)** had instead been **98**, then the Password Generated would be: **2}mAwQGwtL%ci1o**

If, for any reason, you just don't "like" a generated password, then just use a different Sub-Key.

The five choices for generating a password are:

- (A) Numbers Only
- (B) Uppercase Letters Only
- (C) Lowercase Letters Only
- (D) Upper Case Letters, Lower Case Letters, and Numbers Only
- (E) All characters from ASCII 33 through ASC 126.

For the last choice (E), if there are no duplicates then there are still 77 characters that can be used even with not using all the above 17 illegal characters:

$$126 - 33 + 1 = 94$$

$$94 - 17 = 77$$

The total number of 15-character passwords would be:

$$77 \times 76 \times 75 \times 74 \times 73 \times 72 \times 71 \times 70 \times 69 \times 68 \times 67 \times 66 \times 65 \times 64 \times 63 =$$

4,613,384,664,391,550,379,171,840,000 possible passwords.

The total number of 8-character passwords would be:

$$77 \times 76 \times 75 \times 74 \times 73 \times 72 \times 71 \times 70 =$$

848,416,382,352,000 possible passwords.

There are two ways of using PASSWORD.EXE: Either displaying on screen the Password Length, Memorized Key, and Application's Sub-Key OR choosing to hide this information from prying eyes by only displaying asterisks. The nice thing about hiding this information is that you can also "fake" some or all of the information by starting off and ending entries with a few <Spaces>. The program strips off all leading and trailing spaces, so the results will not be altered. Obviously, the generated password will always have to be displayed so that it can be either typed into the application or copied to the clipboard and then pasted into the application. To go "backwards" in the program to a previous entry, just hit <Enter> at the prompt.

Password Maker

1. Numbers Only
2. Upper Case Letters Only
3. Lower Case Letters Only
4. Upper and Lower Case Letters Only
5. Upper Case Letters, Lower Case Letters and Numbers Only
6. Upper Case Letters, Lower Case Letters, Numbers and Other Characters
(Choose) <6>

Enter ALL EXACT Characters NOT Allowed OR <N>one: "+,./:;<=>?[\]|~"

Allow Duplicates?: <No>

Hide Following Entries: <N>

Enter Password Length (Maximum = 77, Minimum = 4): 15

Enter Your MEMORIZED Key (Up To A ±7 Digit with Decimals Allowed): 12345.67

Enter Your Application's Sub-Key (3-Digits MAXIMUM, ≥0): 89

-BD0XpwoHFuUzr7

Hit <Esc> to Quit

Password Maker

1. Numbers Only
2. Upper Case Letters Only
3. Lower Case Letters Only
4. Upper and Lower Case Letters Only
5. Upper Case Letters, Lower Case Letters and Numbers Only
6. Upper Case Letters, Lower Case Letters, Numbers and Other Characters
(Choose) <6>

Enter ALL EXACT Characters NOT Allowed OR <N>one: "+,./:;<=>?[\]|~"

Allow Duplicates?: <No>

Hide Following Entries: <N>

Enter Password Length (Maximum = 77, Minimum = 4): 15

Enter Your MEMORIZED Key (Up To A ±7 Digit with Decimals Allowed): 12345.67

Enter Your Application's Sub-Key (3-Digits MAXIMUM, ≥0): 98

2}mAwQGwtLzci1o

Hit <Esc> to Quit

Password Maker

1. Numbers Only
2. Upper Case Letters Only
3. Lower Case Letters Only
4. Upper and Lower Case Letters Only
5. Upper Case Letters, Lower Case Letters and Numbers Only
6. Upper Case Letters, Lower Case Letters, Numbers and Other Characters
(Choose) <6>

Enter ALL EXACT Characters NOT Allowed OR <N>one: "+,./:;<=>?[\]|~"

Allow Duplicates?: <No>

Hide Following Entries: <Y>

Enter Password Length (Maximum = 77, Minimum = 4): **

Enter Your MEMORIZED Key (Up To A ±7 Digit with Decimals Allowed): *****

Enter Your Application's Sub-Key (3-Digits MAXIMUM, ≥0): **

-BD0XpwoHFuZ:r7

Hit <Esc> to Quit

Password Maker

1. Numbers Only
2. Upper Case Letters Only
3. Lower Case Letters Only
4. Upper and Lower Case Letters Only
5. Upper Case Letters, Lower Case Letters and Numbers Only
6. Upper Case Letters, Lower Case Letters, Numbers and Other Characters
(Choose) <6>

Enter ALL EXACT Characters NOT Allowed OR <N>one: "+,./:;<=>?[\]|~"

Allow Duplicates?: <No>

Hide Following Entries: <Y>

Enter Password Length (Maximum = 77, Minimum = 4): **

Enter Your MEMORIZED Key (Up To A ±7 Digit with Decimals Allowed): *****

Enter Your Application's Sub-Key (3-Digits MAXIMUM, ≥0): **

2}mAwQGwtL%ci1o

Hit <Esc> to Quit