

# Guide to Passwords and Password Security

---

## What is a password, exactly?

A password is a string of characters that you give to verify that you are you when you log into a computer system. On most systems, a password is between 6 and 8 characters long. You can use uppercase and lowercase letters, numbers, and symbols in your password.

---

## What is password security?

The main elements of password security are:

Don't tell it	Do not tell anyone your password.
Don't write it	Do not write your password anywhere.
Make it hard to guess	When you decide on a password, make sure that it cannot be guessed.
If in doubt, change it	If you think there is even a chance that someone else might know your password, change it.
Enter it in privacy	Make sure that no one is standing near you when you enter your password.

---

## Guidelines for good passwords

### Do not ...

Use dictionary word	<b>DON'T</b> choose a password that can be found in a dictionary.
Use public information	<b>DON'T</b> choose a password that uses public information, such as your government ID number, credit card number, phone number, birth date, or driver's license number.
Use family information	<b>DON'T</b> choose a password that uses public information about your family or friends.
Use combined words	<b>DON'T</b> choose a password that is made up of two or more words that can be found in a dictionary, in any form or combination.
Reuse old passwords	<b>DON'T</b> reuse old passwords.
Use user ID	<b>DON'T</b> use your global user ID, or any variation on your user ID, as your password.

---

- Use similar passwords **DON'T** use a new password that is very similar to your old password. If the new password is too similar to the old one, the system may reject it.
- Give out password **DON'T** give your password to **ANYONE**. Sharing accounts is not only against your User Agreement, but it may be illegal as well. Anyone claiming to be systems staff who requires your password is trying to deceive you.

## Do ...

- Avoid significance **DO** choose a password that has no easily discerned significance to you. For example, singer Michael Jackson would not want to have THRILLER as a password because a computer criminal might guess it.
- Use 8 characters **DO** choose a password that is at least 8 characters long.
- Use 3 types of chars **DO** use a password that has at least:  
– two alphabetic characters (a-z, A-Z)  
– one numeric (0-9)  
– special (punctuation) character, e.g., comma (,), period (.), hyphen (-).
- Your password should contain at least 3 different types of characters from the choices above (lowercase a-z, uppercase A-Z, numbers, special characters).
- Use upper/lower case **DO** use both upper- and lowercase characters. Passwords are case-sensitive.
- Memorize password **DO** memorize your password. If you write it down—anywhere—someone could find it and use it to wreak havoc in your name.
- Use completely new **DO** choose a completely new password every time you change.

## Why is password security important?

There are people (known as “Evil Crackers”) who can do awful things to any information stored in your account after they get your password. Even worse, they may be able to do awful things to the accounts of other people, or even break into systems across the world. So the argument “I don’t need a good password; I don’t have anything in my account anyway” does not work. **Security your responsibility.**

## Why can’t I tell anyone my password?

You don’t know where the information will go after it leaves your lips. Even if you only tell one other person, that person could tell one other person, and so on, until your password is in the hands of an Evil Cracker. Besides, why do you want to tell someone your password? On

most systems, you are not supposed to share your account with others. So there is no legitimate reason for them to use your password.

## Why can't I write down my password?

You don't know where the information will go after it is on paper. A password written on a piece of paper is simply too easy to lose. And someone might be watching the next time you take out that piece of paper to log in. Better to just remember your password.

## How do Evil Crackers guess passwords?

Your password is stored on the system in *encrypted* form. It has been run through an encryption math algorithm. There is no algorithm that will take a password in encrypted form and give back the original password. Not even the system administrator knows your password. So Evil Crackers can't find out your password just by asking the system.

Instead, they use a program called Crack to breach password security. The Crack program works by taking strings of characters and encrypting them, then comparing the encrypted text against your password in encrypted form. If the two encrypted versions are the same, then the string of characters is your password.

It would take way too long to simply try every combination of letters you could have as your password — over 100,000 years on a reasonably fast machine. So Crack tries the most likely combinations. First, it starts with everything it can find out about you on the system, like your login name, your full name, your address, your Social Security or other government ID number. Trying all of these takes a few seconds.

Then it moves on to a huge “dictionary” containing words from all languages, place names, people names, names of characters in books, jargon, slang, and acronyms. It tries all of them as your password. This takes several minutes. After Crack is done with that, it tries variations on those words, such as:

- any word, written backwards
- any word, with a punctuation character at the end
- any word, with a punctuation character at the beginning
- any word, with a punctuation character in the 3rd character place
- any word, replacing all t's with 3's
- any word, capitalized
- any two words, put together with a number between them

and so on. It tries every combination you can imagine. So since you don't want Evil Crackers to crack your password, **never use any password based on a word.**

## Tips on how to remember passwords

You're probably wondering how you will ever make a password that you can remember.

There are tricks to creating a good password that can't be guessed, yet can be remembered. Here's one of the tricks: take a phrase you like and will remember. Now use the first letter of

each word. Add any appropriate capitalization, punctuation, and other character manipulations.

Examples:

Phrase that is easy for you to remember	Password based on phrase
Soccer is my number 1 favorite sport.	Simn1 fs.
I see you, you see me too	Isy,ysm2

## Other suggestions: pattern-based passwords

### *Using normal keyboard*

Another tip for generating passwords that are not dictionary words, that follow the guidelines, and that are easy to remember is to generate your passwords using physical patterns on the keyboard. Specify a pattern for the key selection, a pattern for using the **Shift** key, and designate the initial key for the password. As long as your pattern includes at least two keys from the top row of a normal keyboard, you can ensure inclusion of numbers and symbols (with **Shift** key applied to one).

Examples: Type each of these examples yourself to see the pattern on the keyboard:

- V-pattern: 1qaZzse4
- V-pattern with Ab-shifting: !qAzZsE4
- V-pattern with aB- shifting: 1QaZzSe\$
- V-pattern with Abc- shifting: !qaZzsE4
- V-pattern with abC- shifting: 1qAzzSe4
- Reverse V-pattern: 4eszZaq1

You can develop your own patterns of X, A, Z, W, L, U, N, M, box and add more complexity by incorporating alternate-hand typing patterns and mirror images.

### *Using keyboard and number pad patterns*

Another set of patterns results from using a left-hand pattern on the keyboard area and a right-hand pattern on the numeric keypad, such as this: q7z1r9v3.

For added security, keep a set of two, three or four different patterns in your head. When it comes time to change passwords, change to an alternate pattern as well as a new initial key.

Important: If you teach this pattern technique to others, do NOT tell them your favorite patterns! If they know your pattern, they can easily run through an exhaustive set of that pattern with each possible initial key on the keyboard.

### ***Additional information about password patterns***

If you are interested in learning about other methods of designing uncrackable passwords, see the following articles:

**How to Make Windows 2000 and NT 4 Passwords Uncrackable:**

<http://sysopt.earthweb.com/articles/win2kpass/index.html>

**User-friendly and secure passwords:**

[http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci775702,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci775702,00.html)

**Mnemonics – Figure Alphabet:** <http://freespace.virgin.net/mark.farrar1/mnefa01.htm>

---

## **How do I change my password?**

Each operating system (Windows 95/98, Windows NT Workstation, Windows 2000, Windows XP) has a different procedure for changing passwords.

You can usually change your password in all Windows operating systems by using either the Passwords Control Panel or the change password function by pressing Ctrl + Alt + Del.

Changing your password for a website or other application will be done in the application or website.