

Borrowed from Microsoft & SANS Recommendations

Creating strong passwords

Computer security includes the use of strong passwords for your network logon and the Administrator account on your computer.

For a password to be strong, it should:

- Be at least seven characters long. Because of the way passwords are encrypted, the most secure passwords are seven or 14 characters long.
- Contain characters from each of the following three groups:

Group	Examples
Letters (uppercase and lowercase)	A, B, C... (and a, b, c...)
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols (all characters not defined as letters or numerals)	` ~ ! @ # \$ % ^ & * () _ + - = { } [] \ : " ; ' < > ? , . /

- Have at least one symbol character in the second through sixth positions.
- Be significantly different from prior passwords.
- Not contain your name or user name.
- Not be a common word or name.

Passwords are likely the weakest link in a computer security scheme. Strong passwords are important because password cracking tools continue to improve and the computers used to crack passwords are more powerful than ever. Network passwords that once took weeks to crack can now be cracked in hours.

Password cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and automation that will try every possible combination of characters. Given enough time, the automated method can crack any password. However, it still can take months to crack a strong password.

Windows passwords can be up to 127 characters long. However, if you are using Windows XP on a network that also has computers using Windows 95 or Windows 98, consider using passwords not longer than 14 characters. Windows 95 and Windows 98 support passwords of up to 14 characters. If your password is longer, you may not be able to log on to your network from those computers.

Consider using sample phrases as passwords:

The#Quick#Brown#Fox#Ate#1#Rabbit
1ThingIDoEveryDayIsSpend\$
EyeBrush3Time\$Daily
WishIHad247\$

MyParent\$LivedAt128Marshall\$InBoone,IA
GrandpaIs50%Retired
ComputerHelpline(319)273-5555

Advice on creating a strong, but easy-to-remember password that is easily changed:

Build your password around two names that are personal and unusual that are not in the dictionary and you can remember easily such as your favorite uncle's name or nickname and the street or town where he lives. Separate the words with special characters and numbers by starting with pairs of numbers and special characters at one end of the top row of keys and moving to the other as you are asked to change your password. So, for example, you might have an uncle, named "thomas" and he lives in "decorah" (it's easiest to just use all lower case, but capitalizing proper names is easy to remember and makes your password even stronger). Your password could be ")thomas0decorah)". Your next password could be "(thomas9decorah(" and so forth. Or if you start at the other end of the top keys, it would initially be "@thomas2decorah@". If you use up all the numbers you could begin again using "00" "0" or reverse the order of the names ")decorah0thomas)" or pick a new relative or friend, or begin capitalizing the proper names such as "Thomas" and "Decorah", but you only have a small portion of the password to remember.

From SANS:

The best and most appropriate defense against password weaknesses is a strong policy which includes thorough instructions to engender good password habits and proactive checking of password integrity.

1. **Assure that passwords are consistently strong.** Given enough hardware and enough time, any password can be cracked by brute force. But there are simpler and very successful ways to learn passwords without such expense. Password crackers employ what are known as dictionary-style attacks. Since encryption methods are known, cracking utilities simply compare the encrypted form of a password against the encrypted forms of dictionary words (in many languages), proper names, and permutations of both. Therefore a password whose root in any way resembles a known word is highly susceptible to a dictionary attack. Many organizations instruct users to generate passwords by including combinations of alphanumeric and special characters, and users more often than not adhere by taking a word ("password") and converting letters to numbers or special characters ("pa\$\$w0rd"). Such permutations cannot protect against a dictionary attack: "pa\$\$w0rd" is as likely to be cracked as "password."

A good password therefore cannot have a word or proper name as its root. A strong password policy should direct users to generate passwords from something more random, like a phrase or the title of a book or song. By concatenating a longer string (taking the first letter of each word, or substituting a special character for a word, removing all the vowels, etc.), users can generate sufficiently long strings which combine alphanumeric and special characters in a way which dictionary attacks will have great difficulty cracking. And if the string is easy to remember, then the password should be as well.