

Choosing Good Passwords

It can be difficult to choose a good password: the password should be fairly long and shouldn't be guessable, but at the same time it should be easy to remember. If the password is difficult to remember, you will find that you need to write it down. It is not a good idea to write down passwords as someone else can find the paper you have written it on (or the file you have put it in) and digitally impersonate you. Before talking about how to choose good passwords, here are a few reminders of good general password practices:

1) Never share your password.

Your account is assigned to you. You will be held responsible for the activities of the account. We do see cases where people will use someone else's e-mail account to send harassing e-mail. Don't let this happen to you.

2) Never write down a password

Passwords that are written down can be easily stolen.

3) Change your password with some frequency

The longer that you have used your password, the more likely it is that someone else will manage to figure it out. Just how frequently you should change your password depends on how frequently you use it and what you are protecting with it. For example, you may wish to change a password used to give access to financial information more frequently than one to give access to read the news on a web page.

4) Never store your password in a program

Many e-mail clients, web browsers, and web services will offer to store your password for you so that you don't need to type it in each time you want to use it. This is a bad idea -- it is generally trivial for people to recover your password from inside one of these programs if they have access to your computer (and sometimes even if they don't).

It is also possible for some computer viruses to recover your password from such stores and e-mail them to random people or post them publicly on the Internet. Such viruses may even distribute the password before anti-virus software is able to locate and remove the virus.

Methods for Choosing a Good, Memorable Password

General Advice

Please note: For technical reasons, some systems have a fairly short limit on the length of a password. This limit is often eight characters. While the examples below are often longer than eight characters, the concepts for selecting passwords work eight characters just as they do at ten, twenty, or two hundred.

When choosing a password, avoid using dictionary words

Dictionary words are any common words, names, dates, or number, including words in foreign language words. One standard method that is used frequently when attackers attempt to guess passwords is a brute force attack. In a brute force attack, the attacker basically tries possible passwords over and over again until they manage to break into the account. Often they try dictionaries of commonly used passwords. We have seen dictionaries in English, Finnish, German, Japanese, Latin, Spanish, Italian, Chinese, Norwegian, Swedish, Chinese, Yiddish, Dutch, common jargon from Biology, Physics, Computers, common female names, common male names, names from cartoons, movies, television, Shakespeare, religion, mythology as well as common and famous place names. It wouldn't surprise us to see dictionaries of Farsi or Akkadian words, either. Avoid using words or names, regardless of the language.

Don't use common misspellings of dictionary words (*including replacing "l" with "1" and the like*).

Many of the dictionaries include both common misspellings and words with letters replaced with similar looking numbers.

Don't use the name of the computer or your account.

Don't use sample passwords, such as the ones on this page.

Use a mixture of upper and lower case letters, numbers, and punctuation (that is, use multiple character classes 2).

Avoid using characters that don't appear on a standard US 101 key keyboard.

While some systems may allow you to use "unprintables", an accented character, u-umlaut or a Euro symbol, don't count on it working correctly. Characters that aren't easily typable on a standard US 101 key keyboard may not work correctly in all circumstances.

Specific Methods for Selecting Good Passwords

Use letters from a phrase or song lyric.

Think up a phrase. For example, "Marx's Communist Manifesto has 8196 words in it!". Once you've decided on the phrase, choose the first (or last, or the second, or whatever) letter from each word. "Marx's Communist Manifesto has 8196 words in it!"

You'll notice that in this example we've decided to include all the punctuation. This is to improve the quality of the password.

So, your password would be M'sCMh8196wii!. It is a nice, long password with a good mixture of character classes.

Combine a few pronounceable "nonsense" words with punctuation.

For example nuit+Pog=tWi. Pronounceable nonsense words are easier to remember than random characters. In our example we have combined together the nonsense words in a way that is similar to an arithmetic formula which makes it easier to remember. You may want to use other punctuation for similar reasons. Another example might be Fp@par().

Handling Large Numbers of Passwords

In the modern Internet environment, people often find that almost every web site that they visit wants them to remember a password. In addition, most people have passwords to access one or more e-mail accounts and to provide access to all sorts of different Internet-based services that they wish to use. At the same time, using the same password in multiple locations is very dangerous: if the password is stolen from any one of the places where it is used, it can be used elsewhere as well.

Below are a few ideas on various ways to handle the increasing number of passwords that seem to be required these days while not making the passwords easy to guess.

Consider what the password is protecting when choosing a password.

Many passwords protect configuration settings rather than protecting access to sensitive data and/or access to e-mail or other network services. Use a single password for all such services. If the password is not protecting access to any personal or financial information or allows other people to impersonate you (for example, by sending e-mail as you), you probably don't need to keep it as secure. If you are not sure, always use a different password than you use on any other site.

Consider your password as multiple parts: a central core of the password and a prefix and/or suffix which is specific to the service that is being protected.

For example, your core might be "gPw4", from "generic Password 4 (for)..."

If this password is to be a password for the New York Times Web Site, you might choose to add "NYt" to the beginning of the password and "n" (for "news") to the end. This would make your password: NYtgPw4n. Your password for eBay might be eBgPw4A ("A" for "auctions"). The passwords protecting your most sensitive information should always be different than other passwords.

Choose a formula such as the ones described above for the passwords that are less important and typed infrequently, but for the most important passwords choose something that is in no way related to any other of your passwords.

1. While receiving a new password or passwords you may wish to write down your password until that you have a chance to memorize the password or passwords. If you do this, you should take extreme care not to lose the paper you have written it on. You should destroy the paper (e.g. tear it to shreds) once you have learned the password or passwords.

2. Various Character Classes:

Character Class Name Examples

Uppercase Letters ABCDEFGHIJKLMNOPQRSTUVWXYZ

Lowercase Letters abcdefghijklmnopqrstuvwxyz

Numerals 0123456789

Symbols !@#\$%^&*() -+= _|\ `~ [] {} <> ,. " ' ; (etc.)

"Unprintables" space tab control codes