

CHOOSING A GOOD PASSWORD:

What are Good Passwords and Why Do I Need Them?

Today, computer crackers are extremely sophisticated. Instead of typing random password by hand, crackers use personal computers to make connections repeatedly to test passwords in an effort to penetrate security. Even a modest home computer with a good password-guessing program can try thousands of passwords in less than a day's time. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that someone else might guess is a bad choice.

What Passwords Should I Avoid?

- Avoid using your name, your spouse's name, your parents' names, or your pet's name as a password.
- Other bad passwords are these names spelled backwards or followed by a single digit.
- Also avoid things that are listed elsewhere, like your address, zip code, phone number, Social Security Number, Driver's License Number, License Plate number, etc. Remember all of these are likely accessible by the public and can therefore be used to crack passwords.
- Short passwords are also bad, because there are fewer of them and are more easily guessed.
- Especially bad are words from computer games.
- Other bad choices include phone numbers, characters from favorite movies or books, favorite drinks, or famous people.
- Words in the dictionary.
- Words in any dictionary.
- Your user name.
- Your real name.
- Your spouse's name.
- Anyone's name (crackers don't necessarily know that your aunt's middle name is Agnes, but it's easy enough to get a list of 100,000 names and try each one).

Version	Date	Author(s)	Comments
1.0	4/30/09	Eric Graves	

- Any word in any "cracking dictionary." There are lists of words that crackers use to try to crack passwords: passwords that a lot of people use. Some of these lists include:

Abbreviations, Asteroids, Biology, Cartoons, Character Patterns, Machine names, famous names, female names, Bible, male names, Movies, Myths-legends, Number Patterns, Short Phrases, Places, Science Fiction, Shakespeare, Songs, Sports, Surnames

- Any of the above, with a single character before or after it ("8dinner", "happy1").
- Any of the above, capitalized ("cat" --> "Cat")
- Any of the above, reversed ("cat" --> "tac"), doubled ("cat" --> "catcat") or mirrored ("cat" --> "cattac").
- We used to tell people that taking a word and substituting some characters (a 0 (zero) for an o, or a 1 for an l) made a good password. This is no longer the case. New crackers have the capability to crack things like this, in certain situations.
- Words like "foobar", "xyzy" and "qwerty" are still just plain words. They are also popular passwords, and the crack programs look for them. Avoid them.
- Any of the sample passwords, good or bad, mentioned in this document.

Helpful Tips for Choosing a Good Password.

- Include digits and punctuation characters, as well as letters.
- Choose something easily remembered so it doesn't have to be written down.
- Use at least 8 characters. Password security is improved by having long passwords.
- Use two short words and combine them with a special character or a number, like ROBOT4ME or 2MATO4YOU.
- Put together an acronym that has special meaning to you, like NOTFSWFM (None Of This Fancy Stuff Works For Me) or ALPEGCAN (All Law Professors Eat Green Cheese At Night).
- In general, a good password will have a mix of lower- and upper-case characters, numbers, and punctuation marks, and should be at least 8 characters long. Unfortunately, passwords like this are often hard to remember and result in people writing them down. Do not write your passwords down!
- The license plate rule: take a phrase and try to squeeze it into eight characters, as if you wanted to put it on a vanity license plate.

Version	Date	Author(s)	Comments
1.0	4/30/09	Eric Graves	

- Some people like to pick several small words, separated by punctuation marks of some kind.
- Put a punctuation mark in the middle of a word, e.g., ``vege%tarian".
- Use some unusual way of contracting a word. You don't have to use an apostrophe.
- Avoid control characters. A lot of them have special meanings. If you use ^D, ^H or ^U, for example, you might not be able to log in again.
- Think of an uncommon phrase, and take the first, second or last letter of each word. ``You can't always get what you want" would yield ``ycagwyw". Throw in a capital letter and a punctuation mark or a number or two, and you can end up with ``yCag5wyw".
- Deliberately misspelling one or more words can make your password harder to crack.
- Use several of the techniques above.
- Something that no one but you would ever think of. The best password is one that is totally random to anyone else except you. It is difficult to tell you how to come up with these, but people are able to do it. Use your imagination!

Tips on safeguarding your password

- First and foremost, NEVER give your password to anyone. ``Anyone" means your coworkers, your spouse, your systems administrator. In the event of an emergency, the IT Help Desk can change your password. Your system administrator or IT Help Desk rarely has a need to know your personal password. If someone needs to get onto your machines, and has a reason to be here, do not give them access to your account. Speak to the IT Help Desk staff about setting up an account for them.
- Make your password something you can remember. Do not write it down. If you really, honestly forget your password, we can easily give you a new, temporary one. We'd rather set your password once a month because you forgot it than have someone find it written down and gain unauthorized access to your account.
- Make your password difficult for others to guess. This is not as hard as it initially seems. See the section above on choosing a good password.
- DO NOT Change your password because of mail from someone claiming to be your systems administrator, supposedly needing access to your files!! This is a popular scam in some circles. Remember, your systems administrator never needs your password for any reason. If someone needs to ask you to change your password so that they can gain entry to your account, they do not have reason to be there.

Version	Date	Author(s)	Comments
1.0	4/30/09	Eric Graves	