Password Protection
System Security Begins With You

There are two classifications of individuals who try to break into computer systems -- hackers and crackers. Hackers are individuals with proficient computer skills who exploit weaknesses in system programming in order control a computer system. Crackers break into computer accounts and damage the system using the privileges that are available to the stolen account or use the stolen account to mask their identity when attempting to break into other computer systems on the local network or the Internet.

How can these renegades be foiled? The hacker is stopped by closing down the “holes” the s/he finds. Computer Services regularly installs software patches to close down security holes and continuously monitors possible break-in points. The cracker is stopped by good password security and good password security is in your hands.

Keep your password secure.

Never tell someone else your password. Richard Stockton College feels so strongly about this aspect of password protection that it is specifically stated in the acceptable use policy in Standard 2.

“Users may not disclose the password of an account or otherwise make the account available to others who have not been authorized to use the account. Users are responsible for all usage of their accounts and are expected to take appropriate safeguards to assure that their passwords are not known to others.”

Never write down your password. Anyone observing your login will see where it is located and can retrieve it for their use -- or misuse -- when you aren’t around. Even if they don’t observe your login, they will look for anything written down and posted in the vicinity of your workstation (e.g., the side of the monitor, bottom of the keyboard, on the keyboard tray.).

Never send your password to someone else in an electronic mail message. You cannot be sure of the security measures taken on the systems that your message passes through or the security of the system where your message is delivered.

Never use software that automates your login. This type of feature embeds your password into a configuration file or programmable keyboard key. Anyone sitting at your computer has immediate access to your password.

Use a password that you can type easily and quickly. This will thwart anyone attempting to get your password by watching over your shoulder as you type.
Change your password regularly

All of our central systems and file servers require you to change your password every ninety days. If you suspect someone might know your password, don’t wait for it to expire. Change it immediately!

You should change your password more frequently if you TELNET to Stockton’s computer systems from another site. The Internet is a complex web of computer networks and security levels vary. At less secure sites it is possible for a really determined cracker to monitor communications packets and capture your username and password.

Avoid password pitfalls

Don’t pick a password that can be found in the dictionary. Our central computers check your password against a system dictionary, but there are many different dictionaries available. A word that is not in our system dictionary just might be in the crackers’ dictionary. This includes foreign language dictionaries as well.

Don’t choose a password that uses personal information that someone could easily find out about you. This includes information such as:

- Your name, username, or nickname
- Names or nicknames of friends, relatives, pets, or locations that are special to you
- Numerical data about you such as birth date, social security number, license plate number, phone number, address, or zip code
- Technical terms or names of prominent individuals in your field of expertise
- Variations of any of these (e.g., your nickname spelled backwards)

Don’t choose a password that others might also choose. You should avoid:

- Names of famous people such as sports figures, literary characters, mythological figures, biblical figures, actors, or political figures
- Names of computer systems or software products
- Any commercial brand names
- Names of cartoon characters or science fiction characters (especially Star Trek and Tolkein)

Remember, the cracker wants to get into your account with as little trouble as possible. In addition to using dictionaries and password cracking programs, crackers also share lists of common passwords. The words below were extracted from a commonly
used password list published on a cracker bulletin board. None of these types of words are likely to be in a dictionary, but a cracker will try them.

albany  bacchus  batman  beethoven  beowulf  berkeley
berlin  celtics  charon  daemon  disney  egghead
einstein  euclid  ferment  forsythe  fourier  gabriel
garfield  harvey  ingres  kermit  macintosh  merlin
michael  mozart  napoleon  newton  orwell  osiris
phoenix  pierre  polynomial  rachmaninoff  snoopy  socrates
toyota  wombat  yosemite

In addition to the types of words already mentioned, there are also non-words that should be avoided. Don’t use strings of all the same character, for example XXXXXXXXXX. Don’t use numeric patterns such as 246810. Don’t use keyboard patterns such as QWERTY or YTREWQ.

Choose a good password

What is a good password? A good password is one that is easy to remember but hard to guess. There are several methods you can use.

You can use real words as long as you use them wisely. One method is to concatenate two unrelated words. Example are LAMPFISH or BOATAPPLE. Another method takes this idea a step further. Use two common words, but separate them by a non-alphanumeric character. Examples are SPIDER_STAR or SILVER$BOOK. A third method is to intentionally misspell a word or words. For example, the word TEACHER could become TEECHUR.

You can create a pseudo-word by alternating consonants with one or two vowels. These words are pronounceable and easy to remember, but hard to guess. Examples are BOUGAMIT or EXOJUK

Finally, you can create a password like you might create a mnemonic device. Take a phrase that you can easily remember and use the first character of each word. If possible, include numbers and non-alphanumeric characters. For example, the phrase “Four score and seven years ago” could translate into the password 4SA7YA.