

Guidelines for Safe Passwords

Passwords are your keys to computers

A password and username work together as a “key” to a computer system providing specific access for a given user. Access to confidential information, whether coursework, administrative data, or e-mail, is protected by the password/username pair. Thus, it is one of the most critical elements of system and data security. All of the efforts of system administration staff are useless if passwords are not protected properly. A large number of security problems stem from improper protection of passwords and computer accounts. How to select a good password, and keep it secure, will be discussed here.

1) DON'T GIVE YOUR PASSWORD TO ANYONE.

Passwords are initially created as random numbers. The password must be changed immediately on the first access. After that, you **and only you** should know that password.

- Don't write your password down; especially in a place that someone might look for it (inside a desk drawer, under a phone or keyboard, next to the monitor, on a desk leaf, in a wallet, etc.) Commit your password to memory as soon as possible. If you must write a password down, keep it in a sealed envelope in a secure location, and change it when the envelope is opened. Never send a password in email.
- Don't share your account password with anyone, regardless of how well you think you know them. A user account is a privilege granted to a specific person, and sharing that account is a violation of University policy. Even if they're your best friend, your one true love, they are not entitled to use your account. Besides, sometimes even the best relationships turn sour, and then you don't want your new enemy to be able to send email out in your name.
- Never divulge your password to people who purport to be system management or technical personnel. Real system managers don't need your password--the system grants them access from their own account, and will track access as them for all critical activities. If your password doesn't work for some reason, they do not need the old password to change it. **Anyone telling you they need your password for any reason is lying.** Never tell your password to any technical staff. If C&NS employees or network support staff need you to log in to your account, they will do it in your presence and ask you to type in your password when it is needed. You should never leave a person using your logged-in account unattended.
- **DON'T GIVE YOUR PASSWORD TO ANYONE.**

2) Make your password easy to remember, but hard to guess or determine by "brute force."

Avoid using simple English words. Common system attacks involve going through standard dictionary words as passwords. You should also avoid passwords having anything to do with you, like your name, birthday, address, Social Security number, pet's or partner's name, shoe size, basically anything about you that is potentially public knowledge. Avoid these in both forward and reverse order. Avoid sample passwords you've seen in any book or movie. Avoid passwords that are all letters, or only all numbers--such passwords are much easier to have a program guess by trying all possible combinations of such things.

So, what are you left with? The kinds of things that make good passwords are things that have no obvious pattern or no contiguous words. Breaking up words with numeric digits or punctuation is very helpful. Use acronyms or abbreviations of long phrases can also be useful. It is important to select something that can be remembered mnemonically, yet when typed seems to be complete gibberish. Use at least six characters. You can use letters, numbers, uppercase and lowercase characters.

3) Change your password often.

So, you do 1) and 2) above, so why should you need to change your password. It's secure, right? Not exactly. Despite everyone's best efforts, passwords can still be compromised:

- If you dial in on a phone line or login over the Internet, the password data passes through numerous public networks. There have been reports of people compromising network machines and stealing username/password combinations to systems by monitoring signals on communication lines, and thus gaining access. Even if passwords are encrypted, clever criminals can sometimes replay the encrypted sequence.
- If you type a password with other people in the room, they may be able to watch your keystrokes. It's the same as people at pay phones using calling cards and unscrupulous people stealing the card number by watching people key it in. (It's proper etiquette to look away from the keyboard or screen while someone is typing in their password.) If you suspect someone has seen you type in your password, change it immediately.
- It's possible that systems or software you use (mail packages, Web pages, etc.) will store your password in an unencrypted format, or in a format known not to be secure. If this is true, and the system is compromised, those passwords will be made available to the infiltrator.
- Passwords do expire every 90 days by default, but you can change your password at any time.
- You can not use the past 12 passwords when creating a new one.

4) Use different passwords for unrelated systems.

If someone gains access to a computer system, and gets your password, it is then available for their use. If all of your computer accounts use the same password, then they've gained access to all of your computer accounts. While it is easier to remember just one password, it's far more dangerous. Your passwords don't have to be completely different, they can be related, but they shouldn't be identical (or simple permutations like password1, password2, etc.) Having the same password on multiple computer systems means that all of your computer accounts are as secure as the least secure of the systems on which you have accounts. While University servers store passwords in a very secure format that cannot practically be decoded, other sites may simply store passwords in plain text. This means that not only is the password compromised if the remote system is broken in to, but that the administrators of that system can see all the passwords. This especially is an issue with passwords you use for Web access to services--these should be completely different than University passwords or passwords to any data you trust. Use harder-to-guess passwords for your more critical accounts.

You now have the same password for the network, email, remote access, and file sharing. Although this may seem to be a contradiction of the above rule, the difference is that all of these systems will be managed under a common security policy, and passwords will be stored in one database on the network. This model is secure when managed properly and administered by a central organization. Your network and StagWeb account should be two separate passwords.

5) Is this all really necessary?

You might say, "Well, I don't really have anything important on the network, so why should I care about my password?" Even though you don't have sensitive data in your own account, the fact that you have an account on the network means that you are given rights to other files that are confidential to course materials or administrative information. If you're faculty or staff you have shared network space that is writable by you, and that data is very important to others in your department. If your account is compromised, it may be used as a stepping stone to accessing other files or systems, or possibly as a way to attack other systems on the Internet. While these suggestions may seem like paranoia, they are critical in the interconnected, shared Internet to keep not only you but the University safe from unauthorized access.

Password Memory Tricks

Granted, many people have a hard enough time remembering simple words, let alone made-up ones, but there are several ways to teach yourself to remember quickly and effectively any number of bizzare sequences you come up with. The best method for creating a password you don't have to write down is to use an acronym for something in your own experience; for example, I lived in Alaska for five years = iliAf5y.

When Selecting A New Password Do Not Use

- Your first, last, or middle name or a nickname.
- The first, last, or middle name or nickname of your spouse, child, parent, close friend, coworker, or boss.
- A combination of your initials and other parts of your name.
- The name of your pet or any fantasy or cartoon character.
- The name of your department or an abbreviation for your department.
- The name of the operating system running on your computer.
- The hostname of your computer.
- Any name at all.
- Your phone number or license plate number.
- Any part of your social security number.
- Your logon id.
- Your birth date or the birth date of any friend or relative.
- Any other information that might be easily obtained about you, such as your address, job title, or alma mater.
- Any word in the English dictionary or any foreign dictionary.
- A geographical or product name, or any other proper noun.
- An acronym or any technical term.
- Common patterns of letters from the keyboard, like 'aaaaaa' or 'qwerty'.
- Any name or word spelled backwards.
- Any name or word with some or all of the letters capitalized.
- Any name or word spelled backwards and with some or all of the letters capitalized.

- Any name or word with a number, punctuation mark, or other keyboard character added to the front or back of it.
- Any name or word where some of the letters have been changed to a number or other character. Some of the more common ones are:
l changed to 1
o changed to 0 (zero)
a changed to @ or 4
s changed to \$ or 5
- Any name or word with all the vowels removed.
- Two or more small words concatenated together.

Logging out of your account

If you don't log out of your account, the next person who sits down at the workstation has access to all your files. Not logging out is just as dangerous as giving your password to someone.

To log out from a workstation

1. Select the "Start Menu" and then "Shutdown" from the drop down list. OR
2. Use the keystrokes "CTRL + ALT + Delete" to bring you to the windows security dialog box. Select the "Log Off" button.

Note: Logging off your computer will close all of your open programs. Make sure you save your work before logging off.

Locking Your Computer

You can "lock" your computer screen without having to close your programs and logging off your computer.

To lock your computer:

1. Use the keystrokes "CTRL + ALT + Delete" to bring you to the windows security dialog box. Select the "Lock Computer" button. OR...
2. Use the keystrokes "windows key + L" to immediately lock your computer.

To unlock your computer, simply use the keystrokes "CTRL + ALT + Delete" again and login via your network account.