

# Managing Your Andrew Account Password

This document contains the following sections:

- [Your Andrew Account and Password](#)
- [Selecting a Strong Password](#)
- [Forgot Your Password](#)
- [Changing Your Password](#)

---

For information related to this topic refer to:

- [Andrew Account Types \(http://www.cmu.edu/computing/accounts/index.html\)](http://www.cmu.edu/computing/accounts/index.html)
- [AFS and Cyrus Quota \(http://www.cmu.edu/computing/doc/accounts/quota/index.html\)](http://www.cmu.edu/computing/doc/accounts/quota/index.html)
- [Setting a CMUname \(http://www.cmu.edu/computing/doc/accounts/cmu-name/index.html\)](http://www.cmu.edu/computing/doc/accounts/cmu-name/index.html)
- [My Files and Roaming Profiles \(http://www.cmu.edu/computing/clusters/profiles.html\)](http://www.cmu.edu/computing/clusters/profiles.html)

*Last Updated: 10/04/07*

## Andrew Account and Password

Your Andrew account (Andrew ID) is your gateway to the computing environment at Carnegie Mellon. Your account gives you secure access to e-mail, network registration and other services. You can find the Andrew ID of Carnegie Mellon affiliates by visiting the [Carnegie Mellon directory web page \(http://www.cmu.edu/directory\)](http://www.cmu.edu/directory). For more information on requesting an account and specific account entitlements, please see the [Andrew Account Types \(http://www.cmu.edu/computing/accounts/types/index.html\)](http://www.cmu.edu/computing/accounts/types/index.html) page.

## Your Andrew Password

Once your Andrew account has been created for you, you'll need to set a personal, strong password (see the section [Selecting a Strong Password](#)). Depending on your affiliation, refer to the information below:

- **New first-year undergrads who reside in the continental United States and have NOT previously held an Andrew account:** Visit the web page at <https://webiso.andrew.cmu.edu/cgi-bin/passr/initialsetup.cgi> (<https://webiso.andrew.cmu.edu/cgi-bin/passr/initialsetup.cgi>) follow the on-screen instructions to set your password. You'll need to know the Admission ID that you used through the enrollment process to access this web site.
- **All others:** Your initial password will be set to the first eight digits of your university ID. Visit the My Accounts tab of the [Carnegie Mellon Web Portal \(https://my.cmu.edu/\)](https://my.cmu.edu/). Under Password, select the link to [Change Your Password \(https://www.cmu.edu/myandrew/auth/q?loc=webiso&doc=password-change/\)](https://www.cmu.edu/myandrew/auth/q?loc=webiso&doc=password-change/). Next, under Password, select the link for [Forgot Your Password? \(https://webiso.andrew.cmu.edu/passr/\)](https://webiso.andrew.cmu.edu/passr/) and click **Configure...** to configure the password reset tool. Setting this tool now will make life much easier for you if you ever forget your password.

## Why having a strong password is important

Many users believe that having a password which is easy to type or remember is more important than security. Often this is because they are not particularly concerned about the confidentiality of the files in their Andrew accounts. Frequently we hear people say, "There isn't anything important in my account, and I believe in free access to information. I don't really care if someone can break in and get to my files."

While it may be true that their files are not important to them, these people are not considering the larger picture. An account is more than just a collection of your files. When an unauthorized person gains access to your account it can lead to any of the following activities:

- **Send electronic mail as if they were you.** While this may seem harmless at first glance, there have been cases where falsified electronic mail has caused real damage. Such messages can include death threats, fraudulent offers for services or sale of merchandise, or inappropriate or harassing remarks to someone with which you regularly correspond, or to a complete stranger. Further, if you are in a

position of authority (e.g., faculty member, staff member with supervisory duties) falsified messages telling a student or employee that they are going to fail a class or be fired can be presented. There is no way to prove that someone else sent such messages if they authenticated themselves to the system as you, using your password.

- **Read your electronic mail.** This would, of course, include any messages which you consider to be confidential.
- **Use your account as a "launching point" to initiate attacks against other computer systems.** Should such activity occur, you could lose access to the account, and your ability to login, for days or even weeks while your account is examined for the hackers code and hidden files and directories. In extreme cases, your entire account may be copied and given to authorities under a court order.
- **Gain access to other services.** This might include course materials through Blackboard, your grades and registration information, network registration, or other information.

The password to your account is the last line of defense against a potential intruder. Maintaining good password security is as important, and as easy to do as locking the door to your house or your car. A truly determined attacker will find ways to break-in, but making it easy for them is not in your best interest

*Last Updated: 10/04/07*

## Selecting a Strong Password

To avoid problems with other users breaking into your account, you should change your initial password to something more secure as soon as possible. On an ongoing basis, we recommend that you continue to change your password at least once each semester.

When selecting a password, your goal is to make it as difficult as possible for someone to guess. By doing this, you leave a password "cracker" with no other alternative but to search through every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete. There are some simple guidelines, which if followed, would force a cracker to conduct such a search.

Periodically, Computing Services runs a password cracker utility. The password cracker inspects users' Andrew passwords and automatically emails those individuals who use insecure passwords. The password cracker detects passwords with the following vulnerabilities:

- all numeric passwords
- passwords that are comprised of one or more words that can be found in a dictionary
- passwords that are comprised of any dictionary word with a number prepended or appended
- passwords that are commonly found proper names

## Guidelines for selecting a more effective password

Follow these guidelines to select a more effective password. Please do not use any of the examples in this document as your password; "crackers" can read these files and may target specific examples:

- **Do** change your password. Initially, all students, faculty and staff members have a password set for them. You should change this password to your own unique string as soon as possible.
- **Do** create a password that is at least eight characters long and is a combination of upper and lowercase letters as well as numeric values or special characters. Avoid simply changing the case of the first or last letter as this may be insufficient to prevent password guessing.
- **Do** change your password often. We recommend a new password once per semester.
- **Do** choose a password that is easy to remember so you don't have to write it down.
- **Do** choose a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- **Do** use a system for formulating passwords that makes them easier to remember such as:

- o Choose a line or two from a song or poem, and use the first letter of each word. For example, In 'Xanadu did Kubla Kahn a stately pleasure dome decree!' becomes 'IXdKKaspdd!'
- o Choose a password that alternates between one or two consonant and one or two vowels. This provides nonsense words that are usually pronounceable, and thus more easily remembered. Examples include 'root+Boo', 'quaDpop57', 'mOotop75c'.
- o Choose two short words and concatenate them together with a punctuation character between them. Examples include 'dog;Rain', 'book+mug', 'kid?gOat', etc.
- o Choose a collection of words that formulate a sentence such as 'my Pa55word is Strong!'

## Don'ts for Selecting an Effective Password

- **Don't** use your name, your user ID, or the name of a spouse, child, friend or pet.
- **Don't** use information easily obtained about you, such as license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- **Don't** use a password that is comprised of all digits, or all the same letter.
- **Don't** use a word contained in any dictionary, spelling list, or other word list in any language.
- **Don't** use a simple transformation of a word such as reversing the spelling, changing upper-case to lower-case or vice versa, or using all capitalization.
- **Don't** use a password shorter than eight characters. Use a longer number and you'll increase the number of possible password combinations a cracker has to guess.

*Last Updated: 10/04/07*

## What to do if you forget your password

Forgot your password? You may request a password reset in one of the following ways:

- **Use the Password Reset Tool on the Carnegie Mellon Web Portal.**

Visit the My Accounts tab of the Carnegie Mellon Web Portal and click the Forgot Your Password link under Password.

**Note:** You can use this tool only if you have previously configured your confidential questions and answers. If you have not preconfigured Password Reset, you will need to perform one of the other methods provided below.

**OR**

- **Visit the Computing Services Help Center in Cyert Hall 119.**

Make sure you bring a photo ID along with you to the Help Center so one of the consultants can verify your identity and reset your password. Acceptable forms of ID are: Carnegie Mellon ID card, State issued driver's licence or identification card, passport (US or foreign).

**OR**

- **Send a request to reset your password by fax.**

If you are unable to visit the Help Center because you are traveling, you can fax a request to the Computing Services Help Center at 412-268-9773. Please include the following information:

- o copy of a valid photo id
- o signed note requesting a password reset
- o an alternate email address or phone number where you can be contacted

**Note:** Once you send your request, call the Help Center at 412-268-4357 or send email to [advisor@andrew.cmu.edu](mailto:advisor@andrew.cmu.edu), to notify us that you have sent a fax. A consultant will verify your identity and reset your password once your fax is received.

**OR**

- **Contact your department password administrator.**

Faculty and staff members can contact their department's password administrator and have that person request a password reset. The Help Center maintains a list of administrators and can direct you to the appropriate person.

*Last Updated: 10/04/07*

## Changing Your Password

The easiest method of changing your password is via the Change Your Password link on the Carnegie Mellon Web Portal. Follow these steps:

1. From the My Accounts tab of the [Carnegie Mellon Web Portal \(https://my.cmu.edu\)](https://my.cmu.edu), click on the **Change Your Password** link under **Password**.
2. Enter your:
  - Andrew userID
  - Current Password
  - New Password
  - Re-enter your new password to confirm, then click Change Password.

**Note:** You can also change your password via Kerberos for Windows or Kerberos for Macintosh. For more information, see the [Kerberos Authentication \(http://www.cmu.edu/computing/doc/software/kerberos/index.html\)](http://www.cmu.edu/computing/doc/software/kerberos/index.html) page.

*Last Updated: 10/04/07*