

Stronger Passwords

Tips and Guidelines for Creating More Secure Passwords

Overview

This guide is designed to provide strategies and tips for creating account passwords that are “stronger”, as well as relatively easy to remember.

Password Requirements

These rules for stronger passwords are currently enforced for Parnassus, Homer Admin and e-mail, but are recommended for all other systems as well. The password rules are as follows:

- Must be eight or more characters
- Must consist of a combination of letters, numbers and one or more of these special characters: ! (exclamation point), % (percent sign), * (asterisk), + (plus sign), - (dash or minus sign), ? (question mark), _ (underscore)
- Cannot contain the username for that system
- Will expire every 120 days
- Cannot be a password that has been used within the last 18 months

The sections below suggest various methods for creating secure passwords that are fairly easy to remember.

Favorite Lyrics/Phrases/Sentences

Think of a song title, phrase, or sentence that is easy to remember. Using the example "Stairway to Heaven", by Led Zeppelin, the first line of that song is "There's a lady who's sure all that glitters is gold." Take the first letter of each word to get Talwsatgig. Add a number and special character to create an acceptable password.

Combine Small Words

A combination of small common words with a special character and number mixed in makes a secure password that is easier to remember.

Character Replacement

In this method, one or more letters is replaced with a similar looking number and special character. For example, **Apple** becomes **4pp!e**, **Gleam** becomes **6!eam**, or **razzle** becomes **ra22!e**. When used with an 8-letter word this technique generates a seemingly random string of characters that is easier to remember.

What NOT to Do

The following guidelines should help protect passwords from being compromised.

- DO NOT share passwords with co-workers, friends, or relatives
- DO NOT write passwords on a sticky note, notepad, or anything stored in or around monitors or desks
- DO NOT store passwords in unencrypted or plain text files on a computer
- DO NOT let others watch a password as it is typed

For More Information

For additional help, contact the ITS Helpdesk at helpdesk@ithaca.edu or 4-3282.

Copyright ©2008 Ithaca College - All rights reserved. This publication may be duplicated in its entirety for use in not-for-profit educational settings. All copies must include this copyright statement. Any other use requires permission from Information Technology Services at Ithaca College, 607-274-1000, its@ithaca.edu.

Quick Guide