Password safety: Best practices

Last Modified on 08/04/2022 11:01 pm EDT

This article reviews basic **password creation and storage guidelines.**

See also:

- Password Managers: Overview
- Two-Factor: Getting Started with Duo

Overview

Sharing your Bryn Mawr College password with anyone (including family and friends) is a violation of the Acceptable Use Policy ▯.

Your College password allows you access to and ensures the protection of many on-campus services. It locks your computer which, when you log in, gives you access not only to the hard drive, but also your network drives, including your personal drive and any departmental or shared folders to which you have access. It keeps others out of your email and calendar, protecting your communications, personal data and address book. The tips provided here will help keep your password, and therefore your information, safe.

Anyone who has access to your password can access any Bryn Mawr College system you have access to, putting you at risk. You are legally liable for anything that is done through your account, even if you were not present.

Giving people (sometimes unintentional) access to your accounts exposes you to a risk of identity theft, snooping, or taking actions on your behalf.

Guidelines

1. Use a password that is difficult for people to guess.
2. We recommend the use of passphrases — whole sentences complete with punctuation (but no spaces). These are more secure than normal passwords and easier to remember.
3. If your password *must* be written down, store it in a secure (locked) place.
4. **Do not share your password with anyone.** This includes family, friends and coworkers. If it feels like you must, ask us — there is always another solution.
5. If you think anyone else has access to your password, change it immediately.
6. Be careful about saving passwords on your computer. Not all programs keep your passwords in a secure location, and saving passwords in them can compromise your security. If you don't know how the program saves your password, don't save it.

7. Always **lock your computer** when you leave it, and log out of any public computers. Staying logged in on an unlocked computer is the same as giving your password to anyone who walks by.

Alternative Methods

- You can request a **shared network folder** where you and the individuals you identify can share files without allowing others to have access to this information and without sharing your own credentials.
    - Upon request (and sometimes with a bit of paperwork) research assistants, volunteers, student workers and Haverford and Swarthmore community members can take part in these services.
- Place email to be shared within a folder and share that folder with others.

Questions?

If you have any additional questions or problems, don't hesitate to reach out to the **Help Desk**!

Phone: 610-526-7440 | Library and Help Desk hours▯
Email: help@brynmawr.edu | Service catalog▯
Location: Canaday Library 1st floor