Quick Tips: Password Safety

Your new College Password allows you to access to and ensures the protection of the following systems:

- **Your computer** – the files you save to your hard drive, your preferences, Web browsing history, etc.
- **Your email and calendar** – your communications and your personal address book.
- **Your network storage**
  - Your personal directory on the network and the files contained within.
  - Your department’s shared files, and any shared files to which you may have access for research, centers, projects, or privileged or confidential data
  - The P: drive, which contains PeopleSoft confidential data
- **Virtual Bryn Mawr.**
  - Your paycheck
  - Your grades
  - Your status with the college and other personal information

Anyone who has access to your password can access all of these systems, putting you at risk. You are legally liable for anything that is done through your account, even if you were not present.

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

To keep your password safe, observe the following guidelines:

1. **Use a password that is difficult for people to guess.** Your new College password must be at least 10 characters long, and it must include characters from each of the 3 groups below:
   - Uppercase Letters: A, B, C...
   - Lowercase Letters: d, e, f...
   - Numbers and Symbols: 0, 1, 2, 3... and !@#$%^&*()

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 place.**

4. **Don’t share your password with anyone.** Never, ever, ever. [ask us – there’s always another solution.]

5. **If you think anyone else has had access to your password, change it immediately.**

6. **Be careful about where passwords have been saved 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 go away from it, and **log out from any computer that is public.** Staying logged into an unlocked computer is the same as giving your password to anyone who walks by.

Safe options for sharing data with other community members:

Call the Help Desk at x7440 for more information about the following:

1. **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.
   - **Note:** Research assistants, volunteers, student workers and HC and SC community members can obtain Bryn Mawr accounts, allowing them to take part in these services.

2. **Place email to be shared in a specific folder and share that folder only with others.** Alternatively, request a shared email account for your project, journal, center, etc.

3. **Opt to share your calendar,** either on a “view only” basis, or a read/write basis with others.