Passwords are often the first, and in many cases, the only line of defense against cyber-attacks. Think about every account for which you have a password and the data each password protects. For many of us this can include: Facebook (personal photos), online banking, Blazernet (grades, direct deposit information), and email (sensitive papers, bank statements, other account passwords). Unfortunately, if the password protecting that account and data is weak, then that’s essentially the same as not having a password at all. So in order to better protect your personal information, below are some best practices for creating a strong password.

- **Make passwords unique.** Add something to your password that makes it different for each website or account you use. This way one compromised password won’t allow an attacker access to every other account.
- **Create strong passwords.** A strong password is long (15 characters minimum) and complex that includes upper case (A-Z), lower-case (a-z), numbers (0-9), and symbols or special characters.
- **Avoid obvious dictionary words.** Anything related to your normal life (job, hobbies, pet names, etc.) should be excluded from passwords because an attacker might build a dictionary, or list of potential passwords, tailored to contain words related to information they gathered about you. Also, words like “password” should be excluded.
- **Change your password at least every 90 days.** This technique creates a moving target for someone that’s trying to crack your password. In the event that your password is compromised, change it and consider it retired. Attackers typically keep collections of old passwords that they will routinely test in the hopes that someone reused them.

After reading those tips, many of you are probably questioning your ability to maintain that standard. Trust us, we understand. Having to keep up with so many different passwords, remembering which one goes with which site, and creating new passwords every 90 days can be an ordeal, but **there is hope!** Passwords don’t have to consist of combinations of random characters. Below are a few simple methods to show you how to create secure, complex, and easy to remember passwords.

One way to implement these rules is by using *passphrases* as passwords. Here are some general rules for using passphrases to create a password.

1. Start with a **long phrase** that you’ll remember. This can be anything such as a favorite lyric, quote, or title. For this example we’ll use a line from the UAB Alma Mater:
   ```
   Praise to thee our UAB
   ```

2. Make some **memorable changes** to the passphrase. In our example below, we removed the spaces, added a symbol, and replaced the word “to” with the number “2”.
   ```
   praise2theeourUAB!
   ```

3. Make the **password unique** and memorable. Returning to our example, we’ll add the first three letters of the website where the passphrase will be used and something different like the number of letters in the name.
   ```
   apple.com = App5praise2theeourUAB!
dell.com = Del4praise2theeourUAB!
facebook.com = Fac8praise2theeourUAB!
   ```

Remember: A passphrase system will help you to create strong, memorable, and fairly unique passwords. Try creating your own passphrase system today and be proactive. Do NOT wait until your account has already been breached.
UAB’s BlazerID password minimum length is currently 8 characters with a complexity requirement of 1 character from three of the four ASCII sets (upper, lower, numbers, & special characters) and no expiration interval. These minimum standards are in the process of being updated. Be on the lookout for these changes in the coming months!