Passwords

Passwords Are the Last Line of Defense Between a Hacker and Your Personal Information

Most people use passwords to protect:

- Social media accounts (e.g. Facebook, Twitter, Instagram)
- Personal and corporate devices (e.g. laptops, cell phones)
- Email accounts (e.g. Gmail, Outlook, Yahoo)
- Online banking accounts
- Other third-party accounts (e.g. Amazon, PayPal, YouTube)

Hackers can break your password by:

- Guessing common passwords: *123456*, *password*, *abc123*, and *qwerty* are among the most used passwords.*
- Monitoring Wi-Fi traffic: hackers connected to public Wi-Fi connections may be able to observe all information inputted by others connected to the same Wi-Fi, including user names and passwords.
- Sending phishing emails: hackers could send millions of emails that ask the victim to input their email user name and password.

Bellevue University's Password Policy

We require every university password to:

- Be between 8- and 32-characters long.
- Must contain:
  - At least one upper and one lower alphabetic character (a-z, A-Z).
  - At least one numeric character (0 – 9).
  - At least one special character excluding space, single quote (‘) and pound/hash (#)
- The password cannot contain the User ID or User first-name, last-name, or full name.
- Passwords are treated as case sensitive.
- Password history is set to 5 (cannot re-use the 5 prior passwords).
- Passwords cannot be changed more than once per day.
- Passwords must be changed on initial login to the University system.
- Passwords must be changed at least every 90 days.
- An entry of 3 consecutive invalid attempts (Lockout Threshold) within 5 minutes (Lockout Observation Window) will result in the account being locked for 10 minutes (Lockout Duration).

Please refer to Policy Statement 618: Password Policy

Common Mistakes

Here are some common mistakes people make when creating passwords:

- Simple passwords composed of common words are easy to guess.
  Examples: apple, rowboat, bumblebee, blizzard, password
- Passwords written down on a piece of paper or stored in plain text on a computer may be stolen by somebody with malicious intent.
- Using the same password for multiple websites is like having one key for multiple locks; if it's stolen, the thief can open them all.

Are you guilty of making any of these mistakes?

Password Best Practices

- ✓ Avoid using common dictionary words or proper nouns
- ✓ Never share your passwords with anybody, even if you trust them
- ✓ Keep your passwords secret by storing them only in your head
- ✓ Change your passwords at least once every 3 months
- ✓ Use a different password for every website

Please refer to Policy Statement 618: Password Policy

Reporting and Contact Information

If you have any general questions:

– Bruin Support Services at 1.800.756.7920

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.