UNIVERSITY OF RIO GRANDE AND RIO GRANDE COMMUNITY COLLEGE

RioNET Password Guide

A strong password is essential when hacking programs can guess 10 billion plus passwords per second. https://howsecureismypassword.net/ can be used for testing your password.

Step Complexity and Length –Cracking Time:

- Password – Instantly
  - Words are easily broken by a dictionary attack and should never be used.
- P@$$w0rd – 9 Hours
  - Character substitution is a great way to add Complexity.
- All Lower Case Letters 11 Characters - 1 Day
  - Length is important! The longer the password the harder it is to brute force it.
- RioNET Default (RioNET####) - 8 months
  - Default passwords must be changed as they follow a pattern. The last 4 characters can be broken in less than a 1 second.
- Upper and Lower Case Letters 11 Characters no symbols or numbers - 6 years
- 10 Characters Uppers, lowers, symbols, and numbers -53 years
- 11 Characters Uppers, lowers, symbols, and numbers – 5,000 years
  - High complexity and 9+ length is the best practice.

Simple Tricks:

- password + site:
  - P@$$w0rdRioNET - 16 billion years
    - Don't re-use the same password! By adding the site to the password you can avoid using the same password but keep it simple.
- Add the year and change it yearly:
  - P@$$w0rd2018RioNET -7 quadrillion years
    - Sensitive sites should be changed often.
- Use a passphrase:
  - I$ Th!$ Ju$t F@nt@$y? - 3 septillion years
    - A passphrase can be very hard to crack and can be easier to remember.

Questions – Just Ask Us!

Circulation Desk – Phone: 740-245-7005 • Email: refdesk@rio.edu • Text: 740-214-1989
Campus Computing & Networking – Support@rio.edu – 740-245-7481