# Week 3 Lab: Hands-on Password Practice

Complete the Hands-on Password Lab, as outlined in the instructions document:

W03 Hands-on Password Lab Instructions.docx

Fill out this worksheet. When you are finished, save it, and upload it to I-Learn Canvas to be scored. You may earn up to 50 points for this lab.

## Task 1: Learn to create strong passwords.

|  |  |
| --- | --- |
| For what reasons should you change your passwords regularly? Write at least one reason. (1pt) | So it is harder to guess do to less time of the password being the same. |
| Which of the following are strong passwords? Which are weak?   * 1. MyCatLovesMe   2. myc@t\_lovesme   3. MyC@t\_L0v3sM3!   4. Mycatlovesme   (2pts) | A-weak  B-weak  C-strong  D-weak |
| What makes the strong passwords above strong? Why are the others considered weak? (2pts) | Specal charaters and numbers, both upper and lower case letters |
| What are the most import steps you can take to ensure you have a secure password? (1pts) | No repeats of a charater, the more chaotic the characters the better |

(Details)

## Task 2: Identify sites that can help verify you have a strong password.

|  |  |
| --- | --- |
| What is the new password you invented? (1pt) | J@y\_Sup3r-M0to |

(NOTE: do not actually use this password for anything else! Only use it for this lab exercise.)

|  |  |  |
| --- | --- | --- |
| According to the strength testing sites: how complex is your password?  (2pts) | UIC Password strength test: | The Password Meter: |
| Very Strong | Very Strong |
| According to “How Secure Is My Password?,” how long might it take to crack your password? (1pt) | 2 hundred million years | |
| Paste your screen captures below as evidence of completion. (3pts) |  | |

(Details, screenshots)

## Task 3: Learn to use a password generator.

|  |  |
| --- | --- |
| What generated random password did you get? (1pt) | \*Sv@mUN$6ua-RDx6vnjW |
| Why do you think this random password might be *more* secure than the password you created earlier in Task 2? Also, can you think of any reasons why it might be *less* secure? (5pts) | It might be better but I don’t trust the online site. |
| According to “How Secure Is My Password?,” how long might the generated password take to crack? (1pt) | 42 quitillion years |
| Paste your screen capture below as evidence of completion/ (1pt) |  |

(Details, screenshot)

## Task 4: Install and use a password manager.

|  |  |
| --- | --- |
| What is a password manager and why would you want to use one? (5pts) | A piece of software that saves your passwords and encrypts the stored data, you would use one if you don’t like to remember many different passwords. |
| Did you install KeePass? If not, what password manager did you install? (1pt) | No, and I use many of the ones that are included with the software of my devices’ |
| How much time did you need to input your BYU-Idaho credentials and one other login/password credential into your password manager? (1pts) | Not long like 2 minutes |
| Did you encounter any difficulties using your new password manager? Describe your experience. (2pts) | Nope |
| Paste your screen capture below as evidence of completion. (1pt) | Why should I it would be a brech of sequrity |

(Details, screenshots)

## Task 5: Teach password skills to someone else.

|  |  |
| --- | --- |
| Whom did you teach, and how did you assist them? (4pts) | No one |
| When they tested their password at “How Secure Is My Password?,” how much time was estimated to crack it? (1pt) | Not applicable |
| What did you learn when you helped them install a password manager (or when you compared your password manager to theirs)? What else did you learn from working with them? (4pts) | Not applicable |
| What were your key-takeaways from this lab? What did you learn that will help you in the future? (10pts) | That I am lazy and have a high chance of people getting my info |