# 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) | Because if someone gets your password, then it will be useless because you already changed it. |
| Which of the following are strong passwords? Which are weak?   * 1. MyCatLovesMe   2. myc@t\_lovesme   3. MyC@t\_L0v3sM3!   4. Mycatlovesme   (2pts) | If any were strong id say c, and possibly b.  However a and d are way simpler as they have no numbers or symbols. |
| What makes the strong passwords above strong? Why are the others considered weak? (2pts) | B has a symbol, c has symbols and letters, a has multiple caps, but not much else, and d has entirely lowercase except the first letter. |
| What are the most import steps you can take to ensure you have a secure password? (1pts) | That its not predictable in a common sort of way. If you use something that is of common access to people, or just commonly known that you like, then it is WAY easier to predict the password. Also longer, longer harder. |

(Details)

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

|  |  |
| --- | --- |
| What is the new password you invented? (1pt) |  |

(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: |
|  |  |
| According to “How Secure Is My Password?,” how long might it take to crack your password? (1pt) |  | |
| 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) |  |
| 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) |  |
| According to “How Secure Is My Password?,” how long might the generated password take to crack? (1pt) |  |
| 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) |  |
| Did you install KeePass? If not, what password manager did you install? (1pt) |  |
| How much time did you need to input your BYU-Idaho credentials and one other login/password credential into your password manager? (1pts) |  |
| Did you encounter any difficulties using your new password manager? Describe your experience. (2pts) |  |
| Paste your screen capture below as evidence of completion. (1pt) |  |

(Details, screenshots)

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

|  |  |
| --- | --- |
| Whom did you teach, and how did you assist them? (4pts) |  |
| When they tested their password at “How Secure Is My Password?,” how much time was estimated to crack it? (1pt) |  |
| 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) |  |
| What were your key-takeaways from this lab? What did you learn that will help you in the future? (10pts) |  |