# 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) | You should regularly change your passwords every three months to avoid having your account breached or hacked. |
| Which of the following are strong passwords? Which are weak?   * 1. MyCatLovesMe   2. myc@t\_lovesme   3. MyC@t\_L0v3sM3!   4. Mycatlovesme   (2pts) | I would rank the passwords as c,b,a,d in order of strength. C is the strongest in my opinion as it uses characters, in upper and lowercase, and numbers. This password would be extremely difficult to guess. B is the next strongest as it uses a mix of letters and characters. A would be the next as it alternates between upper and lower case. D is the weakest as it has the least variety. |
| What makes the strong passwords above strong? Why are the others considered weak? (2pts) | Having a healthy mix of characters, letters, numbers, and upper and lower case will help build the strongest passwords. If someone is trying to guess your password, or even was shoulder surfing to get your password, that much of a variety would take someone thousands of more tries to break in. |
| What are the most import steps you can take to ensure you have a secure password? (1pts) | For myself, I first make sure that my password is unique and that I am not using the same password multiple times. Then I want to make the most random password. Think of a phrase of two or three things that have no association. So something like purple banana Bugatti. Then I would randomize the casing, add characters, and numbers. I would end up with something like puRPLeB@N@n@bugatt!389. That looks like a good password that is something outlandish and easy to remember, but hard to guess and hard to shoulder surf. |

(Details)

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

|  |  |
| --- | --- |
| What is the new password you invented? (1pt) | puRPLeB@N@n@bugatt!389 |

(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” | 100% “Very Good” |
| According to “How Secure Is My Password?,” how long might it take to crack your password? (1pt) | “Two hundred sextillion 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) | X\*ya;^hQL4\*Dh!Q/ |
| 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) | This could be more secure; it has a lot more characters and symbols. This is something I would never be able to remember. I could see this being less secure If you were to get one of these as a suggested password, or even if someone stored this in a password holder. I wouldn’t be able to remember this, I would have to store this or write it on paper, and that is where I could lose security. |
| According to “How Secure Is My Password?,” how long might the generated password take to crack? (1pt) | 41 Trillion 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 password manager is something you can use for convivence. This helps store passwords since we have to come up with complex passwords, as well as monitor their health and when they will need to be replaced. |
| Did you install KeePass? If not, what password manager did you install? (1pt) | I used my apple password manager that I have been using. It allows me to see how long the password has been used, as well as if the password could have appeared in a leak or breach in an alert. |
| How much time did you need to input your BYU-Idaho credentials and one other login/password credential into your password manager? (1pts) | I already had this installed. It is very simple. It just takes you entering each username and password. So roughly 30 seconds. |
| Did you encounter any difficulties using your new password manager? Describe your experience. (2pts) | No, I did not. |
| 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) | My girlfriend Corinne. |
| When they tested their password at “How Secure Is My Password?,” how much time was estimated to crack it? (1pt) | 10 years. |
| 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) | I learned that she did not understand how much you need to maintain your passwords. She had been using the same passwords for a long time. She was interested in a password manager, but did not install one. |
| What were your key-takeaways from this lab? What did you learn that will help you in the future? (10pts) | I learned that it is important to maintain your passwords. I also learned that I am pretty good at making passwords that are hard to guess! Personally, I need to go in and change multiple passwords in my password manager, because it shows they appear to have appeared in a leak or breach. I will need to delete my old Facebook account and any other social media I no longer use. |