**#This is what needs to be on the slides#**

**Title, Customer and Technical Advisor**.

Title: Do you remember your password? (corny but its what I got) haha

Customer: Dr. Aviv

Technical advisor: Dr. Aviv

**Team Composition.**

**Juan Afable(CS)**

**Kole Burke (CS)(Team Lead)**

**Hunter Hale(CS)**

**Jelani Williams(IT)**

**Concise Project Overview.**

**We will be implementing a gaming website where users make an account with a username and password in order to answer questions on passwords**

**Website specifications:**

1. **Users will login with a username and password of a specified difficulty**
2. **Users will be asked to change their passwords at specific time intervals**
3. **Users will be asked to login at specific time intervals.**
4. **Users will play the game.**
5. **Users will always have the option to change their password at anytime**

**The purpose of this project is to explore the following questions regarding passwords:**

**Do people change their passwords drastically, or are their passwords similar to their previous passwords?**

* 1. **Every time a user changes their password, we will record how different that password is to their previous password.**

**How well do people remember passwords of varying complexity? How likely are people to reuse complex passwords?**

* 1. **We will require groups to make passwords of varying difficulties and we will see if passwords that are more complex will be more similar to their previous password.**

**What is the correlation between interval of required logins and password memorability?**

* 1. **We will record the times that the user resets the password due to the password being forgotten, and the amount of time between logins.**

**How more likely are people to create strong passwords when more strict password requirements are present?**

* 1. **We will have multiple groups required to make passwords of varying difficulty.**

**Backend:**

1. **Store and secure passwords**
2. **Verify that user,password pair gives user access to correct profile**
3. **Ensure password meets the criteria of password requirements, and analyze true strength of password on multiple variations of password criteria**
4. **Provide data storage and analysis of passwords strength**
5. **Algorithms to test passwords and the correlation between memorability**

**Topical Areas**

1. **Using databases to store passwords and maintain a log of how many times each user has needed to create a new password due to them forgetting it. - (Databases)**
2. **Email notification system that sends reminders to users to log in to our system. - (Web development)**
3. **Web page development that will serve as the interface for the user to log into and compete for the prize. - (Web development)**
4. **Design of password strength metrics. - (Information assurance)**

**Justification**

**The purpose of this capstone is to determine habits of midshipmen changing, maintaining, and remembering passwords. This is to serve the greater purpose of creating strong secure passwords, and if necessary, determine viable solutions to a lack of password memorability and responsibility.**

**Redo workload**

|  |  |
| --- | --- |
| **Team Member** | **Specific growth areas and discussion**  **(explanation of how growth area goes beyond what was covered in prior courses).** |
| **Jelani Williams** | **Django, Password Analysis, Social Outreach** |
| **Juan Afable** | **Django, Password Analysis, Social Outreach** |
| **Kole Burke** | **Django, Password Analysis, Social Outreach** |
| **Hunter Hale** | **Django, Password Analysis, Social Outreach** |

**Functional Requirements.**

|  |  |
| --- | --- |
| **Functional Requirements (only need one for now)** | **Acceptance Test Plan test cases (only need normal and abnormal test case)** |
| **Design Competition based research platform for password questions** | 1. **Password logs user into system.** 2. **User enters invalid character for password.** |

**Required Resources.**

**Customer Meeting Summaries.**

**Customer’s Current Process.**

Ideas for how this project is big:

**We want to set up a competition for midshipmen in order to entice people to participate. The competition will be high scoring game based that changes on a regular basis. The website will store all data that is inputted by the user into a database. The prize will be a gift card/meal somewhere. The data to store will be user passwords and demographics.**

**Every user will make an account with a password of a certain predetermined complexity. The users will then be asked to login via email at certain short medium or long intervals to play the game. On the site, the user will always be given the option to change their password, but they will be notified that they are required to change their password during a certain specified interval. There will also be random warning email notifications telling the user they are required to change their password due to a failed login attempt. This will allow us to analysis how users react to password compromises.**

Ideas for research questions:

**The purpose of this project is to explore the following questions regarding passwords:**

1. **How often do people change passwords/ do people change their passwords more than required?**
2. **Do people change their passwords drastically, or are their passwords similar to their previous passwords?**
3. **How well do people remember passwords of varying complexity? How likely are people to reuse complex passwords?**
4. **What is the correlation between number of logins/time intervals between login times?**

Ideas for implementation:

**The implementation of this project will be a website and database with an email notification system to both login and change their password. We must also establish a good sample of people to actually participate in the game, thus social outreach will be a big challenge. We believe the game aspect such as tetris, or snake would be a good way to attract participants.**

What do we need:

**We need and SQL Database, ITSD information to see if midshipman reuse their passwords. A good game to put in a website and grab participants. A game would preferably have a high score associated with it.**

What will each member do:

**By no means is this assignment of tasks exclusive to each member; however, each member of the group has their specialty. Afable and Williams will specialize in the user interface, and database management. Burke will work on social outreach and email notification system. Hale will work on implementation of metric analysis of passwords, and social outreach. All will work on the implementation of game, password specific experiments. Burke and Hale will reach out to ITSD to measure the midshipmen who reuse their passwords.**

Growth of each individual:

**Afable and Williams have never implemented a website and database using Django. Burke and Hale have never used python, nor have done any work to integrate email to programs. We all have minimal experience on the implementation of games in websites.**

Required resources:

1. Django - programming language created in order to ease the creation of complex, database driven websites.
2. Zxcvbn - used for testing complexity of passwords users select, and if that password meets the required complexity of a password.
3. ITSD- information on the habits of midshipmen pertaining to how often they change passwords.
4. SQL database - used to maintain passwords and usernames for users.
5. Game implementation - creation of a competitive game to keep users participating.

Research?

1. Use Zxcvbn to analyze how strong passwords are depending on much leeway we give users when creating passwords. What set of criteria

# 03SEP18

1. In each users profile we will have time stamps which indicate when a user has changed their password. We will have a function that will determine on average how many days it took the user to forget their passwords.

2. We will have our own string comparer which will test their current password against all previous password and determine how close each password is to the new password.

3. Using zxcvbn as a metric to determine how strong a password is and comparing to the number of times they had to change their password because they forgot it. We will analyze the correlation between the two.

4. Change this. Add What is the correlation between forced password changes and the memorability of a password after a forced password change deadline.

* On the back end keep track of when a forced password change occurs and track how many times a user was unable to remember their password

Overall use line graphs to show when a mando change occurs and each interval of time compared to number of successful logins and failed logins resulting in password reset.

|  |  |
| --- | --- |
| **Functional Requirement** | **Test Plan test cases** |
| Login/GUI:  Users will be able to login and play “tetris”  Which will allow them to compete for Chick-fila | 1.a) User logs in with correct username and password and gains access to their account  **Expect result>** user gains access to their profile  (normal test case)  1.b) User logs in with incorrect user name/password  **Expected result>** user is denied access to account  (abnormal test case) |
| User logs in only at assigned intervals:  User will be able to login only when they are emailed to login. | 2.a) User logs in when they are emailed to log in  **Expected result>** user is given access and allowed to play the game to reach a new high score  (normal test case)  2.b) User attempts to login when they have not been emailed to login  **Expected result>** user is able to see their current high score, but unable to play game and reminded that they can only play when they are emailed to login and play.  (abnormal test case) |

04SPE18

Revised Questions for the project (more specific than before)

1. **Do people change their passwords drastically, or are their passwords similar to their previous passwords?**
   1. **When a user forgets or is forced to change their password due to a mandatory password change we will use zxcvbn to measure relative strength of their newly selected password. We will also be using an inhouse password strength method that will compare the users newly created password to previous passwords they have selected and determine how different or similar previous passwords are to the newly created password.**
2. **How well do people remember passwords of varying complexity? How likely are people to reuse complex passwords?**
   1. **We will have different groups of selected subjects be made to create simple, and complex passwords as a part of our research and we will seek to record how often they forget their passwords by asking them to login on predetermined intervals. Each test group will be given certain parameters regarding required password strength and login intervals in which they will follow in order to collect data on how well users remember passwords of varying complexity. These measures are in addition to the mandatory password change interval: i.e. mandatory login every 10 days for those who change their password every 20 in order to observe the memorability.**
3. **What is the correlation between interval of required logins and password memorability?** 
   1. **We will record the times that the user resets the password due to the password being forgotten using our login interval system, and the amount of time between logins. We will take note of whether or not a user has a simple or complex password and use them to observe any relevant correlations we may find in our data.**
4. **How more likely are people to create strong passwords when more strict password requirements are present?**
   1. **We will observe two test groups in action when it comes to password complexity: simple and complex. Each person will be given**

\*\*ways to present data

http://delivery.acm.org/10.1145/1250000/1242661/p657-florencio.pdf?ip=136.160.90.6&id=1242661&acc=ACTIVE%20SERVICE&key=B318D1722F7F4203%2E90252EFF7ADD4E86%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&\_\_acm\_\_=1536109130\_2037dcea333a25daa063c6fb1e92b88f

\*\*possible questions to ask in the survey

How hard did you find it to memorize your password,

on a scale from 1 (trivial) to 5 (impossible)?

•

For how long did you have to carry around a written

copy of the password to refer to? Please estimate the

length of time in weeks

Do you use the same password for multiple accounts?

How often do you change your password for various accounts (bank, email)?

given the password requirements do you believe you have created a strong password?

How many accounts that require passwords do you currently have that you regularly use?

Have you used this password previously for any account you have?

Do you have a common phrase or password that you use regularly when creating a password?