|  |  |  |
| --- | --- | --- |
| **Problem Solving (A3) Report** | **Topic:** Password Generator/Storage | **Date:** 8/19/20 |
|  | **Contributors:** Oni-Kingsmen |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. Identify a Problem** | **PLAN** |  | **4. Propose & Implement Countermeasures** | **PLAN/DO** |
| * + The standard for storage of passwords is having a document or paper with all the credentials inside.   + It would be more ideal to have access to the passwords in more than one device.   + It’s hard to keep track of passwords for every website/account   + Even if the user uses only one password some websites require an increase in complexity to their password which leads to forgetfulness of the password | |  | * + Create a program/application where the storage of usernames and passwords can be accessed immediately through a computer.   + Create an application that stores all passwords behind one master password     1. The master password would have limited tries.   + Having security questions that would not be case sensitive.   + Having an encryption on each password stored.   + Having each password with different layers of security.     1. User chooses the level of security of each password. | |
|  | |  |  | |
| **2. Set the Target** | **PLAN** |  | **5. Check/Evaluate** | **CHECK** |
| * 1. Create an application that stores all passwords behind one master password      1. The master password could also be fingerprint or face scanner   2. Have it work on multiplatform to allow access to copy paste codes that might be complicated to write.   3. Have it also generate scrambled passwords that are hard to guess.      1. Could also take a password as an input and return it encrypted with a key | |  | What will be my/our criterion to know that it worked?   * Having various tests that the encryption has worked * With each test check that each password was stored correctly and securely * Troubleshooting the master password interface to prevent unintended access   In which ways could it fail to be effective?   * Passwords not safely secured * Encryption system bugged | |
|  | |  |  | |
| **3. Analyze the Causes** | **PLAN** |  | **6. Act and/or Standardize** | **ACT** |
| * + The problem comes from losing or forgetting the location of the paper or document or just making sure the passwords are kept in a secure place that only you have access to.   + The paper or document that stores the password could not be with you   + Can generate extremely complex passwords for websites that deny one that you input | |  | * The system would be optimized in a way that the encryption method of passwords is changed frequently to prevent the theft of data. * Frequently have maintenance of the software to secure the storage of data. | |