**Lesson 1.1 – Introduction to Cybersecurity**

**Activity 1.1.2 Password Protection and Authentication**

1. How could these setting help you safeguard personal information? (Step #4)
2. Record other file extension types that you know along with the application that uses them. If you can’t think of any, ask a classmate or search the internet. (Step #12)
3. Enter Data into the Data Collection Table (Steps

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Password | Guesses | Time |
| Crack one-word |  |  |  |
| Crack one-word (beginning) |  |  |  |
| Crack one-word (end) |  |  |  |
| Average time one-word |  |  |  |
| Crack one-word and symbol |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Make some conclusions about the strengths and weaknesses of different type of passwords based on the time it takes to crack them. (Step #23)
   1. Compare how long it took to search a one-word password and a one-word-with-a-symbol password. How many times longer did take?
   2. Comparing runs that used beginning-of-the-dictionary words, calculate how many times longer the two-word algorithm took than the one-word-and-a-symbol algorithm.
   3. Does the time difference indicate the two-word password is stronger or weaker than the one-word-with-a-symbol password?
   4. What could further improve a password?
2. Save a screenshot of your PowerShell window. (Step #24)
3. How do you think CAPTCHAs are an effective way to distinguish between an automated program and a human?
4. Conclusion
   1. In which part of the Cybersecurity Lifecycle would you place authorization and authentication?
   2. Using a tool such as the password cracking algorithm to discover someone else’s password is almost always ethically wrong and, in most cases, illegal. Describe what you think an ethical use of the tool might be.