6441 Project

**Results**

The starting point of this project was quite simple: I wanted to observe how college students set passwords and identify the overlooked security risks hidden in their habits. Eventually, I received 28 anonymous responses. Subsequently, I used the zxcvbn algorithm to assess the strength of these password, and then checked through the HaveIBeenPwned whether they had appeared in leaked records, so that I can understand how easily "weak passwords" could be compromised, and propose more targeted suggestions for improving daily password security.

Based on my research and analysis, I mainly produced the following contents:

* A detailed report that analyzed the strength of passwords, usage habits, reuse frequency, and leakage situations, and included multiple visual charts that correlated these aspects(Appendix A)
* A three-minute presentation video(Appendix B)
* A password tip poster titled "5 Suggestions on Password Habits", which is compiled based on the common mistakes found in the project. (Appendix C)

Key findings:

* It reveals that those "seemingly complex" passwords may actually be quite weak because their structures are too common.
* It has been discovered that even among students with relatively high technical proficiency, the phenomenon of password reuse is still very common.
* Most people still rely on memory to remember their passwords, but this is neither reliable nor secure.
* Even a "highly secure" password may not necessarily mean that you are truly safe.
* It has been verified that there is a positive correlation between the awareness of tools like HIBP and the users' preference for stronger passwords.

**What did I do?**

The entire project was divided into six steps. Firstly, I designed a concise questionnaire consisting of 7 questions and the questions were focused and easy to answer. After collecting the responses, I cleaned the original data to ensure uniform format and accurate content.

Then, I wrote two Jupyter Notebook scripts: one used zxcvbn to score passwords, and the other used HaveIBeenPwned to check if passwords had been leaked. Based on the analysis results, I wrote the main report, extracting some key findings and common behavioral issues. To enhance students' password awareness, I also created a small tip poster, summarizing 5 most practical suggestions, all based on common errors in the data.

Finally, I recorded a 2-minute video and accompanied it with a page of explanatory slides, trying to make the content concise, easy to understand, and not boring.

**My Challenges and Gains**

Looking back at this project, I have also been reflecting: Could my research truly reflect the password habits of a wider range of users?

After all, the sample size of this survey was only 28, and most of them came from a similar student group. The sample size was small and the scope was rather limited. Although this made my focus clearer, it also meant that the diversity and persuasiveness of the data were limited.

Another minor disappointment is that my choices in analytical tools were also limited. Initially, I actually wanted to test the time differences of different attack methods, but later I realized that I lacked the technical depth and resource support, and ultimately couldn't fully implement this idea.

However, these challenges did indeed bring about real growth for me. When working on data visualization, I began to realize that although some passwords may seem complex on the surface, their structure is still very weak. This made me re-understand "human error" and "security design". And when I was researching the correlation between password reuse and leakage, I gradually understood the trade-off between "usability" and "security" in system design.

Through this project, not only have I become more proficient in using tools like zxcvbn and HIBP, but I have also improved my way of conducting investigations and analyses. I have learned to ask more precise questions. Some assumptions that seemed reasonable at first I now question, and I view the underlying meaning of the analysis results more rigorously. Most importantly, I have realized that truly effective cybersecurity must take into account both technical mechanisms and user-centered education and guidance. Without personally going through this project, I probably wouldn't have such a deep understanding.

Appendices

Appendix A: Questionnaire(15 questions version)

<https://github.com/CyclonneMonster/6441-Project/blob/main/version%20of%2015%20questions.docx>

Appendix B: Questionnaire(7 questions version)

<https://github.com/CyclonneMonster/6441-Project/blob/main/version%20of%20%207%20questions.docx>

Appendix C: Questionnaire(in Chinese)

<https://github.com/CyclonneMonster/6441-Project/blob/main/Questionnaire(in%20Chinese).pdf>