**Reviewer Report of “Rethinking Passwords”**

**Feedback of the article:**

In this article, the author discusses the significance of using strong and unique passwords for all online accounts. The article emphasizes that weak passwords can lead to security breaches and personal information being compromised. The article also provides tips on how to create secure passwords, such as using a mix of letters, numbers, and symbols, and avoiding common phrases or personal information. Overall, this article effectively conveys the importance of utilizing strong passwords for online security. It is a valuable resource for readers looking to improve their password practices. However, it would have been helpful for the author to provide more specific examples and case studies to further illustrate the potential consequences of weak passwords. Additionally, including some information on password management tools or services could have also added practical value to the article. In the first article, it would be amazing to see a more diverse sample of participants. Many participants were university students, and it is possible that their password practices may not be representative of the general population. Additionally, while the article also offers interesting ideas for improving security policies, it would be better if article had more concrete suggestions and examples.

The article could be improved by gathering data from a more diverse population and presenting more concrete suggestions for improving security policies. Additionally, the grammar of the article can be improved by making necessary revisions such as properly using comma placement and verb tense consistency. Evaluating above article, passwords are a widely studied topic in the field of security. The first two sources, from Florêncio and Herley, present research on password management guidelines and common misconceptions about password stealing respectively. The third source, a comic strip from xkcd, humorously addresses the difficulties of creating secure passwords. Overall, these sources suggest that the traditional methods of creating strong passwords may not always be effective in protecting against attacks.

**Summary:**

In the first article, Florêncio and Herley challenge the common belief that randomly generated passwords are secure against attackers. They argue that this belief is not supported by empirical evidence and propose alternative methods for improving password security. The second article discusses the history and origins of security policies, showing how they often fail to consider human behavior and can be ineffective. The third article is a comic strip illustrating the futility of complex passwords in protecting against determined hackers. Overall, this issue presents a critical examination of conventional approaches to password security and offers suggestions for improvement. However, more research is needed to fully understand the effectiveness of these proposed methods.

**Conclusion**

This article could be a valuable resource for readers looking to improve their online security but adding in additional practical advice and examples could enhance its effectiveness. Editing for sentence clarity would also improve the readability of the article. Overall, I recommend publishing this article with revisions. Thank you for the opportunity to review this piece.

References:

Cheswick, W. 2012; http://www.cheswick.com/ches/papers/std-002-results.xls; and http://www.cheswick.com/ches/papers/std-002-results.numbers.