

1. I showed you at the beginning of my speech how easy it is to crack a short password. [Bring up visual aid again.]
2. If we look at the details for the short word we chose earlier, you can see the maximum time and number of guesses the computer would need to make.
3. Now, let's try it again with a long password; can anybody give me a simple sentence? [Enter the sentence into the program.]
4. I will not try to crack this one as it will most likely cause the computer to freeze—instead, I will go straight to the details.
5. Where the short password took only a few seconds to crack, the long password will virtually never be cracked.

B. The second aspect of a strong password, that they should be changed every six months, is also to prevent cracking.

1. In November of 2013, Steve Ragan published an article on the CSO magazine website about an attack on Adobe that exposed more than 130 million accounts (Ragan, 2013, para. 7).
2. Ragan reported that passwords for these accounts were stored encrypted, but not in the best way, so cracking them is still possible (para. 6).
3. Changing your password every six months is the best way to stop someone who has an encrypted copy of your password.

C. The final aspect of a strong password, that they should be unique, is to prevent intruders from gaining access by reusing valid credentials.

1. By unique, I mean that the same password should not be used for multiple accounts, and once changed, should never be used again.
2. Having unique passwords is important because it prevents an attacker from getting all of your important data when one account is compromised.

V. **[Refutation]** Judging by the results from my questionnaire, I do not think any of this is a surprise to you.

A. **[Denying Inherency]** The answer I saw most often for why you don't change passwords every six months or why you reuse passwords for multiple websites was that you were worried you would forget them.

1. Remembering passwords is certainly a challenge, especially when they are long and change frequently, but there is an easy way to overcome this problem.
2. The method I prefer is to use easily remembered sentences made out of random words.
  - a. [Visual Aid] This comic, published by Randall Munroe on his website xkcd.com, demonstrates exactly what I mean.
  - b. Although the password in the first panel looks strong, it is actually rather weak and is difficult to remember.
  - c. The password in the fourth panel, although it appears quite simple, is difficult to crack and easy to remember.

B. **[Minimization]** Another answer I saw repeatedly was that changing passwords took too much time.

1. This is a fair answer; it takes a few minutes to change a password, and when there are multiple accounts that you need to change the time adds up.
2. But consider this: the Federal Trade Commission performed a study in 2003 on identity theft victims (FTC, 2003).
3. In their study, they said the average amount of time an identity theft victim spent resolving their problems was 30 hours, and the average cost was \$500 (p. 7).