Password Practices among Computer Science Seniors at ECSU

James Donahue

Eastern Connecticut State University

<https://jtthe4th.github.io/Senior-Research/>

**Abstract:**

Passwords are a big part of our lives. They are also something that can be taken for granted, given how many people have to remember. Finding the practices used by students could give some insight into what practices people use on a day to day basis. To help understand this a little better, I surveyed a class of students in a Computer Science Senior Research class at Eastern Connecticut State University. As this is far along into a Computer Science major, it was not too shocking that many people used good practices and thought highly of not only the importance of their accounts but also felt confident in their password policy.

**Introduction:**

Passwords serve many purposes in our lives. Whether it’s to get into a building or into accounts a lot of things require passwords in order for them to be accessed. They are one of the main ways that we use to protect our data. The problem with this, however, is that many people create predictable passwords for their data[1]. This can make them vulnerable to being exposed. One is led to believe that users would create strong passwords, knowing what information they can unlock[2]. This is not always the case, and with users having 8.5 accounts[2], this could lead to many problems if passwords are repeated or created poorly.

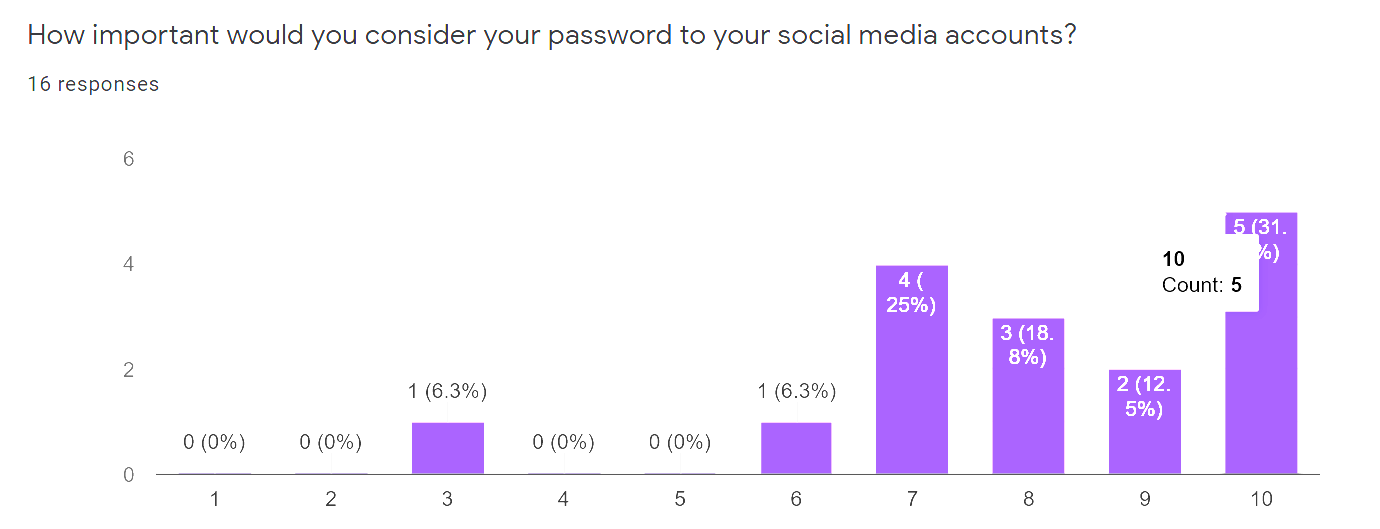
Companies lose $400 billion every year[3]. While this isn’t hackers steal $400 billion every year, it’s that the cost of dealing with hackers in some regard costs companies this much. While this may not show the importance of password policies one should have, it attaches a monetary value to what passwords and other security measures are used in order to keep user information safe. While there is nothing one can do about the security of say a banking institution one uses, they can still employ password practices so that they can at least do everything within their own power to make sure their information is secure.

The goal of this research is to learn about the practices used by students in Senior Research and compare how different and similar they are to their peers, and if password policy they use changes based on how important they deem the account. As user defined passwords are a security measure that will be used for the foreseeable future[4], it is important that users have a strong sense and application in regards to password policy.

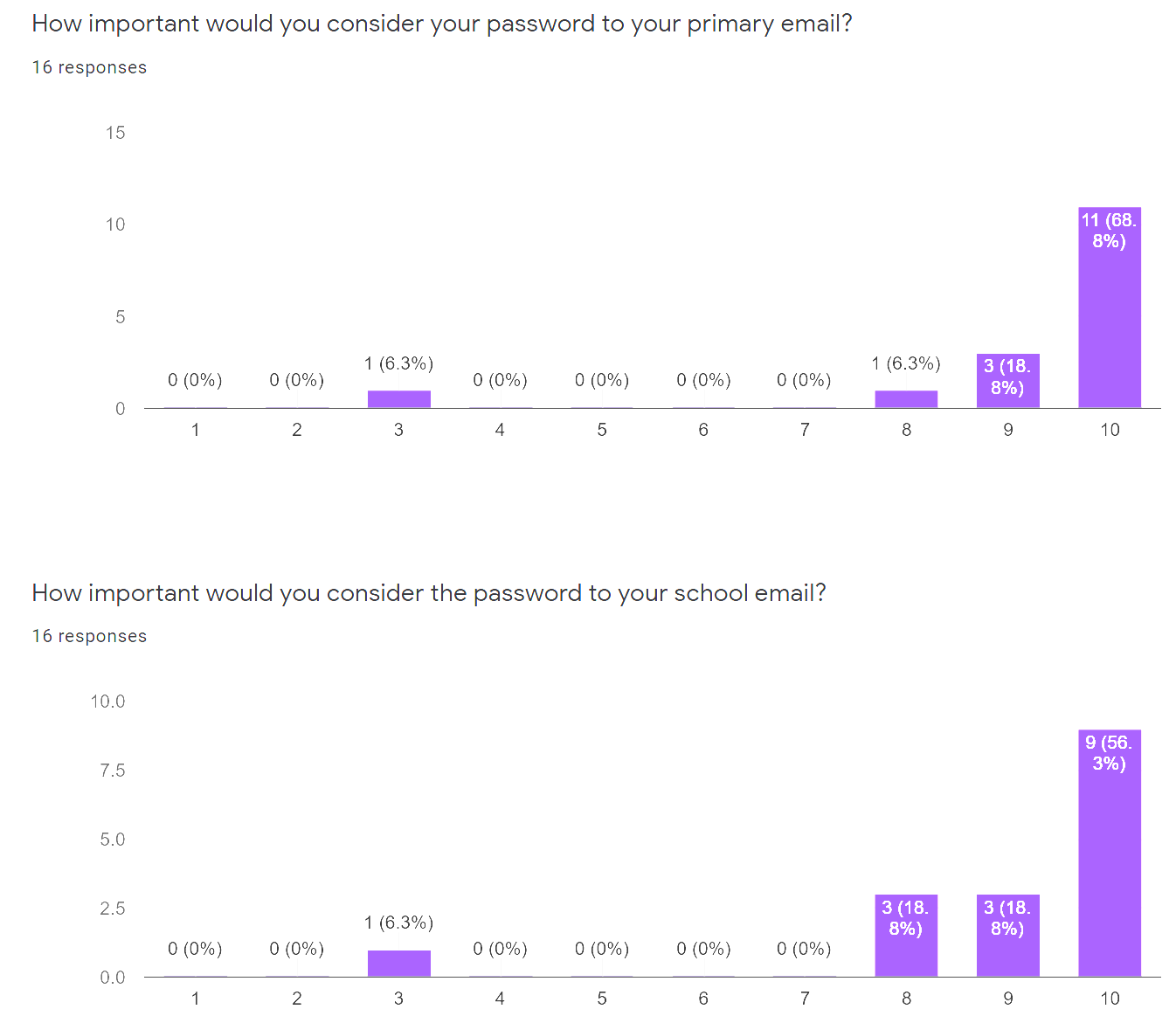
**Methodology:**

Using Google Forms I created a survey for my Senior Research class at Eastern Connecticut State University to answer. Questions range from “How important do you consider the following accounts on a scale form 1-10?” to “Do you use the same or similar passwords for accounts that you consider important and those you do not?”. The survey has been distributed to the class via email to those who completed the consent form. This data was analyzed to find out not only what they consider good or bad policy, or their use of those policies, but also to see if there are areas which results vary significantly enough to be noticeable from the others. Tables and graphs have been made to represent such results. A link to the data is also on the Github page linked in the beginning of this paper.

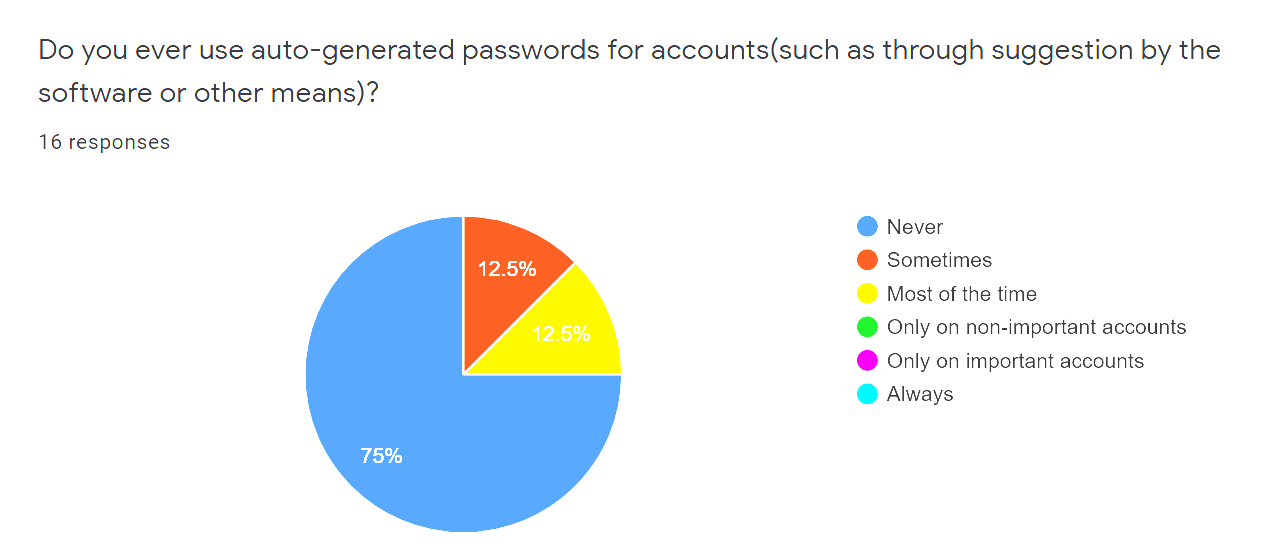
**Results:**



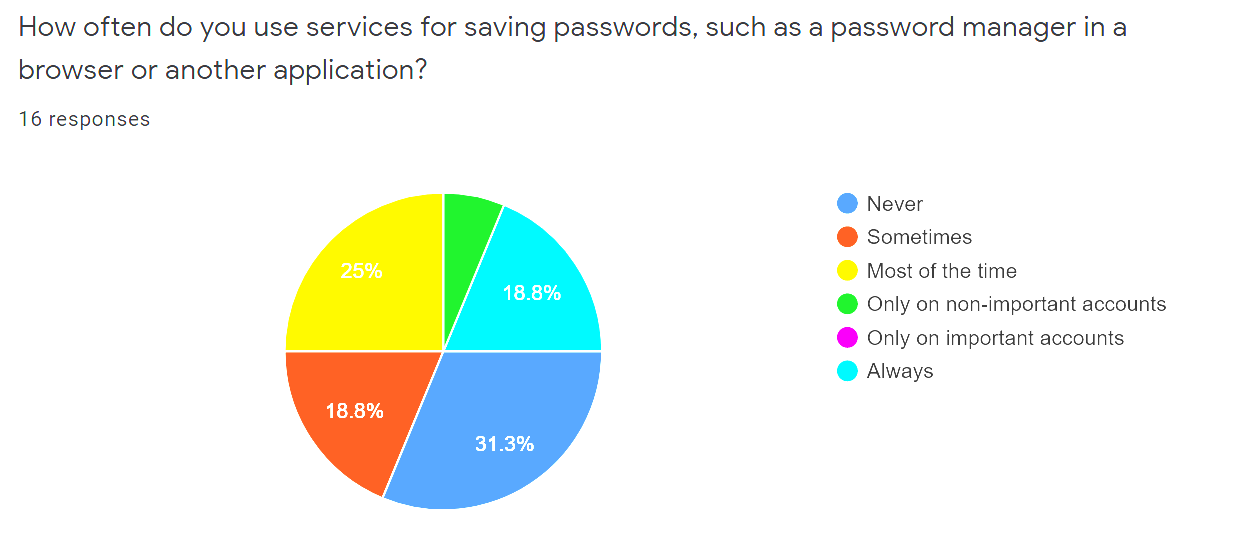
**Figure one** shows the responses to how the students felt about how important their social media password is.



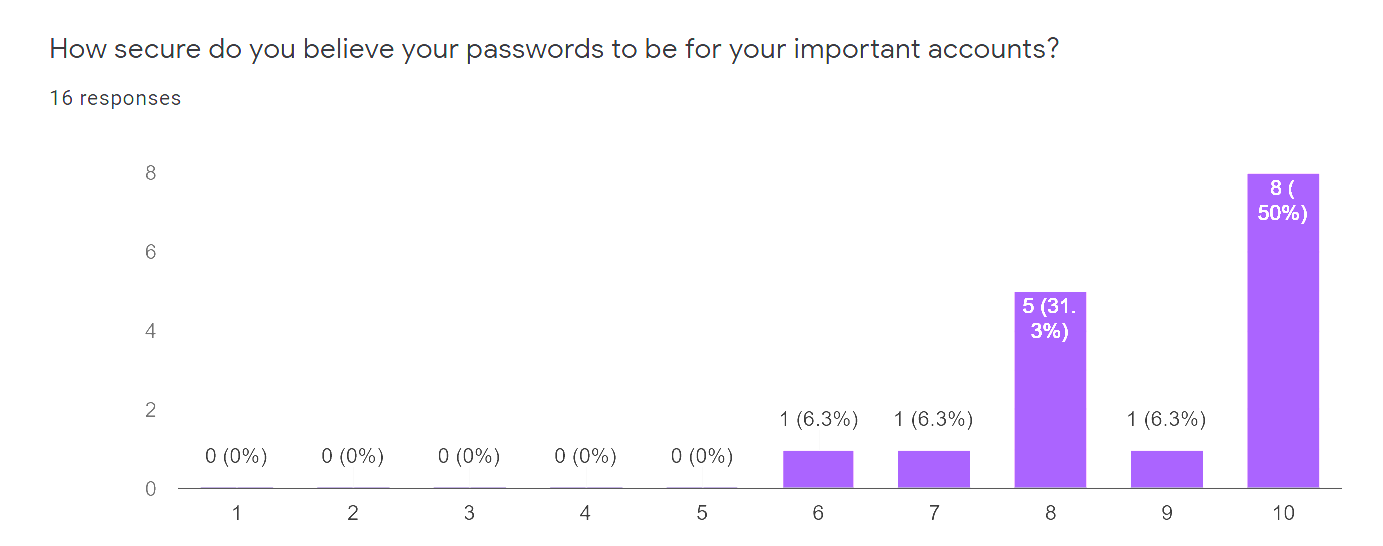
**Figure 2** shows the slight difference between how the students felt between the importance of their primary email account and their school email account.



**Figure 3** displays how often students use auto-generated passwords, recommended by a third party such as a password manager.



**Figure 4** shows how often they use an application, whether it be a browser or password manager, to save their password.



**Figure 5** shows student responses to how secure they believe their password practices to be.

**Discussion:**

As the participants of the study are all in their senior year of their computer science major, it is not surprising that they have a strong concept of password security. It is also unsurprising that they use stronger passwords for accounts they see as being more important. There is still some surprise that the importance of social media account passwords is still rather high, never dipping below halfway.

There is some surprise that password auto-generators weren’t used frequently as show by figure 3, though this may be due to a lack of access to one or a lack of trust in one, neither of which were measured in this study. This could also simply be due to the students having a simple preference of making passwords themselves. Figure 4, showing how often students use some sort of password manager, is not too surprising as there are a lot of passwords one may have to remember, which could lead to ones deemed less important being stored in the password manager and others manually input when needed.

The research I have done is similar to another paper, titled “Security in the wild: user strategies for managing security as an everyday, practical problem”[5]. This research had a much larger survey pool, as they were able to do their interviews at multiple sites and have a data pool from an audience with a much more diverse background. The research done there was not only about the security habits of those in the study, but also delved a bit into the ways in which those interviewed presented themselves online.

Another similar work, titled “Rational Security: Modelling Everyday Password Use”[6], talks about different groups of users, such as administrators or computer scientists, use varying degrees of password security based on the sensitivity of the use it was needed for. This shows that users are at least somewhat aware of what a secure password is and use it when they have to. This paper also talks about the difficulty of remembering passwords, which is a big factor that users have when they create new passwords and can be a reason as to why passwords are reused as often as they are.

This project is heavily limited as the limit survey pool of <20 participants from a single Computer Science class is not enough to represent the habits of an entire major, let alone a university or something more meaningful. This is still important however, as it can give a general baseline to be repeated with a larger sample size and participants of a more diverse background.

**References**

[1] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, “Do Users’ Perceptions of Password Security Match Reality?,” in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose California USA, May 2016, pp. 3748–3760, doi: 10.1145/2858036.2858546.

[2] S. Riley, “Password Security: What Users Know and What They Actually Do,” p. 5.

[3] W. Yakowicz, “Companies Lose $400 Billion to Hackers Each Year,” *Inc.com*, Sep. 08, 2015. https://www.inc.com/will-yakowicz/cyberattacks-cost-companies-400-billion-each-year.html (accessed May 11, 2020).

[4] M. Dell’ Amico, P. Michiardi, and Y. Roudier, “Password Strength: An Empirical Analysis,” in *2010 Proceedings IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5461951.

[5] P. Dourish, R. E. Grinter, J. Delgado de la Flor, and M. Joseph, “Security in the wild: user strategies for managing security as an everyday, practical problem,” *Pers. Ubiquitous Comput.*, vol. 8, no. 6, pp. 391–401, Nov. 2004, doi: 10.1007/s00779-004-0308-5.

[6] G. B. Duggan, H. Johnson, and B. Grawemeyer, “Rational security: Modelling everyday password use,” *Int. J. Hum.-Comput. Stud.*, vol. 70, no. 6, pp. 415–431, Jun. 2012, doi: 10.1016/j.ijhcs.2012.02.008.