Jose Rojas

12/11/23

What do Social Scientists Know About Password Policy

BLUF

Speaking from first hand experience, password policy is a huge deal in cyber security and the IT world. More security for an organization would come with less convenience for their employees, it is challenging to find a perfect balance. Complex passwords would be difficult to type in everyday and take away efficiency as well, but there could be some solutions and policies that could help increase convenience.

Password Policy

Passwords have always been tied together with technology whether it's accessing your personal computer, logging in to work computer, or just accessing your phone. Strong passwords are what gives you the security and privacy you need. The reason I chose this topic is because during my internship over the summer I was introduced to a software that is also web based and it manages all of your passwords. I've done some research and most articles can vouch for this type of approach because it allows more security among passwords and allows user convenience to go up. This is hard to do because normally if the security goes up then the user convenience would go down.

Articles and Research

The first article titled “Four ways to make sure your passwords are safe and easy to remember” talks about trial and error when creating passwords. Its significance is to show that passwords are being used poorly despite Microsoft and Bill Gates predicting that passwords would be gone by 2021. The article also points to the National Cyber Security Center which recommends you use a strong and separate password for your email, to use three random words, save passwords in browsers like Chrome, and to turn on two factor authentication.

In a different article we dive into how balancing cybersecurity and academic freedom is a challenge on campus. This article talks about how different the two worlds are between corporations and universities. Corporations have a much easier time compelling employees to comply with access control policies and universities don't because students are “free-flowing.” It also talks down on two factor authentication because it takes too much time but this is not true as we all use DUO and we know how quickly we can grant yourself access to your accounts. I also want to point out that I have worked with ITS here at ODU and we divide and conquer everything. Overall I disagree with the approach of this article because they want to take out DUO and have less security because of user convenience.

The third article would be “Choose better passwords with the help of science” and this article held experiments on passwords. The experiment would be to crack passwords and test users ability on creating a strong and complex password. The model they created would basically start with words from the dictionary and add the number “1” at the end and go from there. Unfortunately it does not state how many were cracked but it does say that hackers have been able to crack passwords from large companies like Yahoo, LinkedIn and Adobe. At the end it

gives us a set of rules to follow just like the first article did, tells us to use two factor, and to not reuse passwords.

In a different article titled “Time to rethink password changes” written by Lorie Cranor, NIST states that although password change is beneficial it can be ineffective for others and often a source of frustration. As technology continues to advance it is important to keep up with the security challenges that organizations and small businesses can face. It is also important to keep referencing NIST which is the National Institute of Standards and Technology which basically provides us with guidelines on how to choose a password, complexity of a password, and why a password manager could be useful. I want to note that password managers like LastPass are important because this allows you to choose the most complex password and essentially lock it in a vault of passwords. LastPass is a password manager that could work as an extension for your browser and whenever you are prompted to login with something it would pull the password from LastPass. If your computer is compromised you would still need to login to LastPass in order to use it to fill the other passwords, also if you are not using LastPass for 10-15 minutes it will automatically log you out and force you to login. There are downsides to this because if someone not authorized is logged in to the password manager they have the keys to the castle and therefore it is game over.

In the final article “Choosing and Protecting Passwords” written by the Cybersecurity and Infrastructure Security Agency will help guide you in choosing passwords, keeping passwords safe, as well as why you need strong passwords. This could relate to the national and even international level because governments all around the world need to follow stricter rules for password policy. Especially in this time when technology and cyber security are at its peak.

Summary

The articles from the conversation helped a lot in finding problems and solutions to password policy across corporations and universities. Some articles were against DUO and some were for it but when it comes to security organizations should put security before user convenience. The common theme across these articles is that passwords are super important and can cause a huge security breach if not taken seriously. In order to keep good cyber hygiene organizations should be up to date with their password policy as well as properly enforce them.

References

Christin, Nicolas. “Choose Better Passwords with the Help of Science.” *The Conversation*, 13 Sept. 2022, theconversation.com/choose-better-passwords-with-the-help-of-science-82361.

Furnell, Steven. “Four Ways to Make Sure Your Passwords Are Safe and Easy to Remember.” *The Conversation*, 13 Sept. 2022, theconversation.com/four-ways-to-make-sure-your-passwords-are-safe-and-easy-to-remember-159164.

Ryoo , Jungwoo. “Balancing Cybersecurity and Academic Freedom Is a Challenge on Campus.” *The Conversation*, 13 Sept. 2022, theconversation.com/balancing-cybersecurity-and-academic-freedom-is-a-challenge-on-campus-62392.

Ritchie, J. N. & A., Staff in the Bureau of Competition & Office of Technology, Cranor, L., Technology, T. F. O. of, & Nguyen, S. T. (2021a, March 26). *Time to rethink mandatory password changes*. Federal Trade Commission. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2016/03/time-rethink-mandatory-password-changes

Choosing and protecting passwords: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2023b, September 28). https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords