David Sackler

10/5/20

Assignment 1

Synopsis

For my article, I chose Mr. Alan Williams's "Decade of research shows little improvement in password guidance" article. The article starts by talking about how it is concerning how most major brands fail to provide effective advise for creating a password. "Some still allow people to use the word 'password', while others will allow single-character passwords and basic words including a person's surname or a repeat of their user identity." These brands do provide some advice, but most of it is not very effective against cyber attacks or effective against being hacked. The study showed that the top three best brands in terms of providing guidance when creating a password were Google, Microsoft Live and Yahoo. The three worst brands were Amazon, Reddit and Wikipedia. It was noted that there has been a major improvement in the amount of websites that are not allowing the word 'password' as a password. This statement just shows how ridiculous password protection has been. The amount of websites that are offering advice has been slowly increasing, but not at a fast enough rate. The overall story of password protection has more or less been the same since 2007. One major positive has been two factor authentication. Two factor authentication is a shrive that alerts a separate device that someone is logging into your account and requires a code from that separate device to log into whatever is being logged into. This second device is usually a cellular device. The issue is that people require a surprising amount of encouragement to use two factor authentication. So, in practice, even this type of authentication falls short. Password protection is important and currently, the protection it is giving users falls very short. There needs to be improvement in password advice and technologies.

How it applies

The internet has been part of our lives for a while now. It has quickly consumed many peoples lives and jobs. People spend multiple hours of their day scrolling through the web looking at frivolous things that have little affect on their lives. On the other side, people spend multiple hours online for their jobs or accessing personal information. One way that people can protect their information from others is by implementing a password. A password is some sort of key that only the user knows that once inputted, allows the user to access whatever information they have stored. Many websites and applications require passwords to keep user data private and safe. A couple of examples of that would be logging into Facebook or into a Minecraft account. Seeing how ubiquitous passwords are and knowing how important they are to protecting information, it is important that they are effective. The article shows us that passwords have potential to be effective, but they have been implemented poorly. Most major brands give very poor advice for making a good password and even allow the word ’password’ as a password. It is time for a change.

In my opinion, these issues are a result of the creators thinking about theory rather than practice. In previous classes, I have learned that what a programmer thinks he has created does not always transfer to the user. For instance, I could program a website that tells you the weather. However, while navigating to that page is easy for me to do, it might be incredibly unintuitive for someone who is not the creator of the program. That is why it is so important to have multiple stages of user testing. In the case of password, it seems like something that was programmed by a creator that was not passed through many stages of user testing. If it was, most of the issues would have been ironed out. For instance, maybe the creator would have noticed that people use the exact same password for multiple services. Or that people use easily hackable passwords. In recent years, various services have requirements for passwords such as including a number or a capital letter. In my eyes this is not good enough. It is too similar to what we already have. We need a better way of securing information.

There are many ways that this password fiasco can be improved. For instance, AWS uses a great method of protecting user information. AWS requires a normal password, a master password, and that the user downloads a folder onto a computer that is check every time the user logs onto the website. Meaning, the user must go through three different verification steps. Another great way of protecting information is by using a users biology. We see this with fingerprint scanners and facial detection.

In my project, we require a password to protect a users information. We store users personal information in a profile section. This personal information at the moment contains the users progress, account information, and various other personal information. It is important to us that this information is private to the user and it is also important that the user believes that his information is safe. I am unsure of what we are capable of, but in a perfect world, I would like to implement a required two step verification and an optional folder that can be downloaded onto the users device. This would ensure a level of privacy and protection that would allow the user to feel safe. Of course, this is additional to a normal password that the user must enter at each login to gain access to the program. There is no reason that the user should feel that his information can be hacked. Of course, nothing is perfect, but we must try our best.

Article

Williams , Alan. “Decade of Research Shows Little Improvement in Password Guidance.” *University of Plymouth*, University of Plymouth Drake Circus Plymouth Devon PL4 8AA United Kingdom +44 1752 600600 Maps & Directions Visit Us Job Vacancies, 17 July 2018, www.plymouth.ac.uk/news/decade-of-research-shows-little-improvement-in-password-guidance.