Bahar, Talia

6 Oct. 2020

Prof Johnson

CMSI-401

Assignment 1: Article Summary

"Decade of research shows little improvement in password guidance" by Alan Williams, a Media and Communications Officer at the University of Plymouth, details a 2018 study evaluating the password aid given to users across the top ten English-speaking sites on the web. The study was conducted by the University of Plymouth Professor of Information Security Steve Furnell and published in Computer Fraud and Security. Furnell conducted similar evaluations in 2007, 2011, 2014, and much to his dismay he found that most of the top ten English-speaking websites offered little or no advice guidance on creating passwords that are less likely to be hacked across all his studies. Even though the threat of hackers has increased and password cracking technology has improved over the past decade the password protection aid being given to consumers seems to be at a standstill. Furnell goes on to say that, "despite the prospect of new technologies coming into force, [passwords] are still the predominant protection people can use when setting up online accounts."

Furnell's study "examined the password practices of Google, Facebook, Wikipedia, Reddit, Yahoo, Amazon, Twitter, Instagram, Microsoft Live, and Netflix — all top companies that house user sensitive information and data. The study focused on "whether users were provided with guidance when creating an account, changing their password or resetting a password, and how rigorously any guidelines were enforced". Google, Microsoft Live, and Yahoo proved to be the three best sites in terms of account permitted password length and other

restrictions. They were also the top three sites in 2014. The sites that ranked lowest in their password protocols were Amazon, Reddit, and Wikipedia. Notably, Amazon's password requirements "remaining the most liberal". The only improvement he saw was the number of sites that allowed users to set their password to the word "password" decreased. Furnell believes that the availability of two-step verification and two-factor authentication is a step in the right direction but more sites need to be incorporating these methods into their password creation and recovery systems. He goes on to say that users need more encouragement and obligation in terms of traditional password use guidelines. Williams ends the article with 5 recommendations on how users can secure their password: (1) the longer and more diverse characters the better, (2) passwords should not be personal or dictionary words as those are easily guessable, (3) consumers should "not use the same password across multiple accounts and services", (4) passwords should be stored in a safe place and written as hint instead of the actual password, and (5) email passwords are the most important passwords to keep discrete and hacker-proof as password reset and recovery links are typically sent there.

The fact that from 2007 to 2018 Furnell's studies saw little change in password protection support across the top ten English-speaking websites points to a large problem within software development. Software developers need to focus more on the continued protection of their users. Their users might be in their minds in a business and traffic sense especially in early development phases, but once a product is launched how do companies support their consumers and protect them and their data from hackers? Providing users with strick password creation guidelines and implementing two-factor authentication for password recovery does not seem like it would take much manpower or time. Prompting the user on how to make a safe password upon account creation seems especially simple as sites could go as far as adding static text with

recommendations. However, the sites tested are all million-billion dollar companies with gigantic and global user bases. They have the means to guide and protect their user's passwords yet have been failing to do so. I wonder who this responsibility falls under—product designers? software engineers? quality assurance engineers?

The article prompted me to think of how the sites and devices I commonly use handle password protection, creation, and recovery. When creating a new account I have often been asked to provide a combination of letters, numbers, and a special character but this mandated diversity and sometimes password length is not something I consistently encounter. Some sites like MyLMU and Depop require me to change my password every once in a while and do not let me reuse passwords I have used in the past. Furnell's study named Google and Apple as top password protection sites and from my own experiences I can see why. Both Gmail and Yahoo Mail have a two-step authentication protocol for when I reset or forget my password which I like because of the added safety. It also makes it easy for me to access my accounts if I have forgotten my password because I have the option to text myself a verification code. After the article's author highlighted the importance of email passwords I see why Google and Yahoo have stricter password procedures. If a hacker can break into one's primary email than they can easily reset your passwords across other sites as password recovery emails will be sent to that email. All companies with email software should employ strict password procedures and require two-step verification for password resets.

A company not mentioned in Furnells's study that I think does a good job in protecting its users from hackers is Apple. As an iPhone and MacbookPro user, I have the option of using my fingerprint to unlock my devices and those with newer iPhones also have face recognition. Apple's website also employs two-step authentication but it is clear Apple is looking for other

ways to bypass the traditional password methods in order to rival the advancement hackers have made in their own password hacking technology. I would have liked it if Williams' article spoke more about how hackers crack people's passwords, such as what technology and methods they employ. Furthermore, what criteria does a site need to have to make it a target for these hackers? From the 10 companies studied I wonder which sites encounter hackers the most.

I'm also curious to know how these sites handle user password hacking in terms of if a user reaches out to the company's customer care for support about account recovery or closure. The only time I've ever been hacked was through my Uber account. Uber does not have a customer support phone number and my emails were initially responded to with what was clearly an automated response. I could not get into my account because the hacker and changed the password and thus I could also not reset my password without knowing the current changed password. I had to email Uber over 5 times to close my account before I stopped getting and an automated response to just change my password and had an actual employee reached out to tell me my account had been closed. And I haven't used Uber since then. Uber is a mobile app and the study focused on websites so I wonder if different procedures follow for mobile and web platforms regarding password protection. All in all, to keep users loyal and their data secure large software companies need to do better at promoting safe password practices across their platforms and engineer and integrate extensive user authentication methods. From a customer service standpoint to maintain their reputation and credibility these companies also need to create better avenues for password recovery and support.