The Psychology of Cyber Insecurity

Daniel J Westrich

Abstract

There have been a multitude of recent cyber attacks including the Equifax hack, the DNC email hack, and many more. Immediately following announcements of these attacks, individuals and governments alike manifest a visceral reaction of anger and frustration. Everyone promises change, but the fervor quickly dissipates, and very little is done in response to these cyber attacks. This shows a lack of care on the part of individuals and legislators alike for improving overall security. This disconnect is primarily because cyber security is an intangible issue, like online harassment and climate change, and unlike home invasions and murders. Societal problems such as this are much more difficult to solve, as there is simply less desire to solve them. This lack of awareness of intangible issues leads to perpetuation of these issues. With regards to cyber authentication in particular, the vast majority of passwords are relatively easy to crack because they are short, simple and uncreative. These passwords are subsequently hacked, leading to the next security breach, and so on. This issue can be mitigated, however, by increasing awareness of insecure passwords and more secure methods of authentication, as well as by holding those responsible for user security more accountable for allowing cyber attacks to occur.

Introduction

On July 29th 2017, Equifax reported a massive data breach that caused private data for 143 million individuals to become public knowledge. This data includes names, dates of birth, social security numbers, and addresses. Equifax did not publically recognize this hack until September 7th, well over six weeks afterward.[1] Executives at Equifax were subsequently inundated with questions and concerns from the public and from government investigators. For those of us watching this event unfold on our televisions and in our newspapers, it seemed as if the corporate executives would finally be punished for their neglect and that fruitful improvements in Equifax's security apparatus would be implemented. However, this was not the case. Very soon after their initial announcement, spokesmen for Equifax declared that they had conducted their own investigation into the data breach, and concluded that it was the direct cause of one lower-level employee.[2] While the validity of this claim is still in debate, the claim itself caused enough disturbances amongst those angry with Equifax that interest in the truth has subsequently dwindled.

While the Equifax hack is certainly still within public knowledge, the visceral reaction from September 7th has since dissipated. This rational leads to a negative cycle where cyber security violations occur, there is public and federal outcry, and then a return

---

[1] Lee Matthews, "Equifax Data Breach Impacts 143 Million Americans," Forbes, last modified September 7, 2017, accessed December 12, 2017, https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#68188562356f.

[2] Matthews, "Equifax Data," Forbes.

to complicity. Other hacks illustrate this propensity for lack of care. For instance, in 2014 it was announced that White Hat hackers had discovered how to accomplish live mobile phone tracking, using a security bug in the SS7 phone-call routing protocol.[3] Despite this cycle, neither individuals nor governments seem to have an interest in truly solving it. While the rationale describing this irrationality can be complex and multifaceted, in essence, it can be simplified into one particular issue that pervades many other issues involving humanity. People do not care about what they cannot comprehend, and their own cyber security is one of these. Thus, they continue to use insecure passwords and other methods of authentication. This lack of public awareness and care leads to relaxed cyber security policy on the governmental level, thus creating a culture of cyber insecurity. In this paper, I will analyze why there is a disparity between the levels of security that people think they need versus the levels of security that they actually need. I will then describe actionable policy that would mitigate this problem.

To the Community

I chose this topic in order to shed light on one of the fundamental causes of cyber insecurity. Passwords and other methods of authentication are constantly used in order to access our private information. Credentials are used to authenticate banking information, social security information, and a host of other critical private documents and information. If this information falls into the hands of other people, then entire livelihoods can be destroyed. We would assume, then, that people care deeply about ensuring that their data is secure. They would demand that their private data is encrypted, use complex and auto-generated passwords in order to protect themselves from cyber threats. However, this is both quantitatively and qualitatively not the case. Cyber attacks continue to occur, and the list of most common passwords has remained mostly unchanged since they became widely used. Therefore, there is some disconnection between desired security and needed security. It is this disconnection that I am interested in exploring.

Beyond the fact that stealing credentials is a seriously dangerous offense, as described previously, it is also very easy to mitigate effectively. A vast majority of the accounts broken into employ very easily cracked credentials. The top three most common are “123456”, “password”, and “12345678”.[4] These passwords are all, quite obviously, extremely easy to crack. While individuals certainly play the predominate roll in this issue, governments and private corporations can certainly improve their security apparatus as well. Regardless, individuals would save themselves significantly by using

---

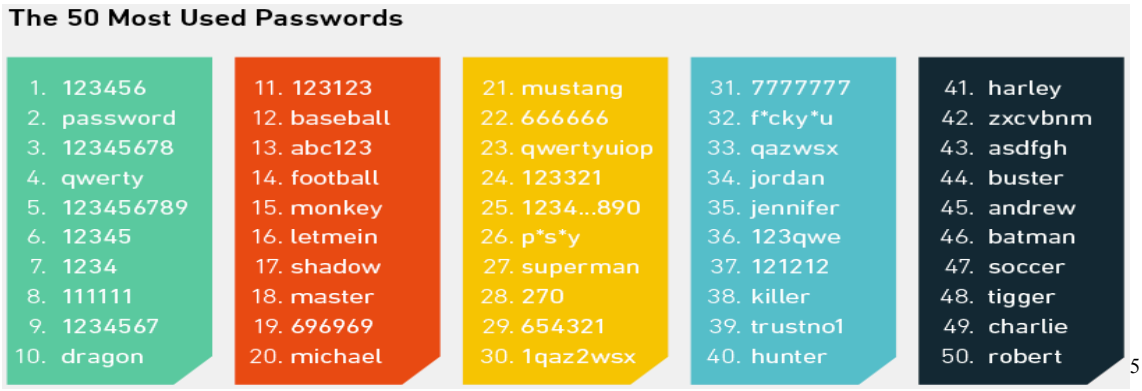
[3] John Leyden and Simon Rockman, "White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln," The Register, last modified December 26, 2014, accessed December 12, 2017, https://www.theregister.co.uk/2014/12/26/ss7_attacks/.

[4] "Unmasked: What 10 million passwords reveal about the people who choose them," wpengine.com, last modified 2015, accessed December 12, 2017, https://wpengine.com/unmasked/?SSAID=1238556&utm_source=SAS&utm_medium=af.

more complex passwords. In essence, blame for the societal lack of care for the security of login authentication is ubiquitous, but there are still things you can do to minimize your exposure to hacks, as I will describe.

Analytics

While it is critical to understand how to improve authentication security, it is equally as necessary to understand the characteristics of good and bad passwords. An analysis of ten million passwords was recently conducted, the data from which will be discussed here. Firstly, let us analyze the top fifty most common passwords used in the study.



[5]

As can be seen, the most common passwords used are almost entirely easily guess-able. For instance, “123456”, “123123”, and “superman” would be cannon fodder for even a simple brute-force credential-finding algorithm, such as John the Ripper. There are other passwords in this last that, at first glance, do not seem obvious. For example, “qwerty” falls into this category. However, these strings are simply linear permutations of keys on a keyboard. The string noted above is simply the first six characters on the top left of a computer keyboard.[6]

Some individuals choose to make their credentials a bit more secure by adding a numerical character as a suffix onto their original password. While this is certainly more effective than not having one, doing this does not improve the security of one’s password by a significantly large amount. This is especially true because the most common extra numerical character, “1”, comprises 23.84% of all numerical suffixes concatenated onto password strings. Other individuals attempt to make their passwords more secure by increasing the number of characters in them. This is one of the most effective forms of password-protection, if done properly. This is because each new character increases the search time exponentially, as all previous searches must be re-done for each permutation

[5] "Unmasked: What," wpengine.com.

[6] "Unmasked: What," wpengine.com.

of the added character(s). Despite this improvement, about 30% of individuals in the study still only have eight characters in their passwords, and about 98% have passwords containing less than twelve characters.[7] One other way to increase credential security is to increase the entropy of a password. Entropy is a scientific term that denotes disorder, and can be explained in a security context to mean the relative disorder of a password. For instance, the string "asdf" has significantly less entropy than the string "adkel#%(@105gP". This is because many password-cracking applications use lists of dictionary words and names to base guesses off of. Passwords with high entropy have less of a chance of being in a dictionary, and thus, on a wordlist.[8] They are therefore much less likely to be cracked.

Given the analysis above, the most secure password would be quite long and consist of many random alphanumeric and non-alphanumeric characters. Since most users have a multitude of different credentials for various websites, it would be extremely difficult for anyone to remember all of their credentials. Thus, it is very difficult for individuals to employ these techniques, and there is a trade-off between a password's security and its usability. This logic, of course, precludes the existence of third-party applications that assist with this problem.

Action Items

As described previously, there is a severe disconnect between the level of security that individuals feel that they need to protect their private data and the level of security that they actually need to do so. There are multiple software systems that are commercially available that would improve the security of user accounts. These services include, but are not limited to, Apple's Keychain, Dashlane, and Two-Factor Authentication. While each certainly provides an increased level of security, none are end-all-be-all solutions. Each has benefits and drawbacks.

Apple's Keychain service and Dashlane are used both to create and store a user's credentials for a copious number of webpages. An individual can use them to store a password that he or she had already formulated, or to create a brand-new password string and store it. There are certain critical benefits of using services like this. Firstly, the user no longer has to remember all of his or her credentials. This allows users to generate passwords with higher entropy than they would if they were required to memorize them.[9] These services also automatically inputs a user's credentials into the appropriate website, making the login process even less strenuous for the user. This is truly the main benefit of

---

[7] Howard Schmidt, "Cyber Security: Securing Our Cyber Ecosystem," *JSTOR*, last modified 2013, http://www.jstor.org/stable/j.ctt13x07xx.21.

[8] Mark Burnett, "Ten Million Passwords FAQ," Xato, last modified February 10, 2015, accessed December 12, 2017, https://xato.net/ten-million-passwords-faq-3b2752ed3b4c.

[9] Daniel Sheehan, "Dashlane Review 2017," Comparakeet, last modified September 27, 2017, accessed December 13, 2017, https://www.comparakeet.com/password-manager-reviews/dashlane-review/.

using a service like Keychain or Dashlane, as it allows individuals to lazily have their passwords generated without having to remember or input them accordingly.[10]

Despite these benefits, there still exist drawbacks, some of which have the potential to severely limit the feasibility of services like Keychain and Dashlane. The primary benefit of these services, that they provide a central location for all of a user's credentials, is also their largest drawback. One issue with this model is that, if the system is hacked, then all of the user's credentials are accessible. If a credential-saving service were not used, then a hacker would have to attempt to retrieve each credential individually. This would take significantly more time, and would therefore dissuade an attacker from attempting. If a service such as this were used, then an attacker would have a much higher reward, and so would spend more effort and energy attacking the service itself.

Another issue with central credential-storing applications is that a user subscribes directly to the accessibility of the program. For instance, if the program requires an update or is experiencing a DDoS attack, then every user's credentials would be unavailable. Also under this argument, once a user commits all of their credentials to a particular service, it can be quite difficult to transfer them to another service is desired. This creates a very price inelastic market for these services. For instance, if service A decided to charge its users an extra dollar in the future, it could implement features that make it more difficult to leave the product.[11] This would cause users to pay more for the product, and would therefore allow these service providers to act as price-makers. This would ultimately dissuade individuals from investing in them, which would be counterproductive.

Lastly, the user must be able to access the application in order to access their credentials. Thus, a user must retain knowledge of a particular password for the service itself. While users are more likely to create a password with higher entropy if they only need one, it would still need to be remembered. It is therefore likely that a user could choose a subpar password, which could then be hacked.

Another form of increased application security is Two-Factor Authentication (TFA). This feature allows users to confirm their identity using a separate device, such as a mobile phone, while logging into websites and such. One benefit of this service is that it adds another layer of security for users, making it more difficult for hackers to break in to. However, since TFA requires the user to interact significantly more with the application before logging in, it is often rejected by users as being too tedious to use. Additionally, TFA provides another layer of security but does not fully blunt hacking attempts. There are examples of TFA being thwarted by hackers in order to gain credential information. For instance, if the secondary check occurs by sending an SMS

---

[10] Lory Gil, "Everything you need to know about iCloud Keychain," iMore, last modified July 30, 2017, accessed December 13, 2017, https://www.imore.com/icloud-keychain.

[11] Sheehan, "Dashlane Review," Comparakeet.

message to a user's mobile phone, that message can be hacked and used to falsify a valid login attempt. There are also examples of TFA being circumvented by hackers who infiltrate phone company records while a user's mobile phone is resetting, allowing the hackers to access the TFA login token and access the user's credentials.[12] While TFA is certainly a useful method of increasing login security, it can lull users into a false sense of security, which can be taken advantage of.

Services like Apple's Keychain, Dashlane and TFA provide valuable means for users to add additional layers of security onto their login credentials. They can be effectively used to combat hackers and protect the integrity of data. However, none are end-all-be-all solutions, and ought not be treated as such. Any individual who employs such systems should be aware of the drawbacks as well as the benefits before fully committing to them.

Conclusion

Large data breaches continue to occur, and individuals continue to use woefully insecure passwords and methods of login authentication. Thus, there is a disconnect between the amount of security that users want and the amount of security that they need. This disconnect is due to inertia, that users simply do not want to remember copious high-entropy passwords or use TFA's additional authentication steps, and catalyzed by the intangibility of the idea of a cyber attack. If people do not see a legitimate problem and do not wish to expend more effort to secure their credentials, then they will not do so. Thus, there must be greater incentives for people to utilize more secure credentials and login methods, as well as more awareness of what a cyber attack is and how it can severely negatively affect individuals. This will not occur naturally, however. Firstly, people only begin to care *after* a tangible crisis has personally affected them *individually*. Secondly, many people do not understand Microsoft Word, Excel, or how the TCP Handshake works, and so perhaps it is unreasonable to expect them to understand the difference between using a random password and adding a few extra non-alphanumeric characters to their normal password. Thus, rather than simply focusing on minimizing the number of these major hacks, we must also prepare ourselves individually by educating ourselves on how and why we should effectively secure our private data. Just as we lock our cars and our homes, we must also protect our computers and our phones.

[12] Brandom, "Two-Factor Authentication," The Verge.

Bibliography

Brandom, Russell. "Two-Factor Authentication is a Mess." The Verge. Last modified July 10, 2017. Accessed December 13, 2017. https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess.

Burnett, Mark. "Ten Million Passwords FAQ." Xato. Last modified February 10, 2015. Accessed December 12, 2017. https://xato.net/ten-million-passwords-faq-3b2752ed3b4c.

Gil, Lory. "Everything you need to know about iCloud Keychain." iMore. Last modified July 30, 2017. Accessed December 13, 2017. https://www.imore.com/icloud-keychain.

Leyden, John, and Simon Rockman. "White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln." The Register. Last modified December 26, 2014. Accessed December 12, 2017. https://www.theregister.co.uk/2014/12/26/ss7_attacks/.

Matthews, Lee. "Equifax Data Breach Impacts 143 Million Americans." Forbes. Last modified September 7, 2017. Accessed December 12, 2017. https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#68188562356f.

Otis, Daniel. "Is there ‘love’ in your online passwords?" The Star. Last modified February 13, 2015. Accessed December 12, 2017. https://www.thestar.com/news/gta/2015/02/13/is-there-love-in-your-online-passwords.html.

Schmidt, Howard. "Cyber Security: Securing Our Cyber Ecosystem." *JSTOR*. Last modified 2013. http://www.jstor.org/stable/j.ctt13x07xx.21.

Sheehan, Daniel. "Dashlane Review 2017." Comparakeet. Last modified September 27, 2017. Accessed December 13, 2017. https://www.comparakeet.com/password-manager-reviews/dashlane-review/.

"Unmasked: What 10 million passwords reveal about the people who choose them." wpengine.com. Last modified 2015. Accessed December 12, 2017. https://wpengine.com/unmasked/?SSAID=1238556&utm_source=SAS&utm_medium=af.