Nathan Brooks

Professor Riddle

English 2010

April 5th, 2015

Responsibility of Users to Protect Their Own Data

There are a vast amount of people using internet technologies on a daily basis, but a surprisingly small number of these users know how their technology works. It is not unreasonable to expect that companies will keep their usernames, passwords, bank account numbers, etc., safe from hackers.

The majority of users do not know the smallest bit about how the internet really works, and almost all agree that they do not know enough to keep themselves safe. Hackers have an easy job when amateurs put their sensitive data out on the internet. This is especially true when companies do not protect data as well as they should.

Part of this problem is due to the fact that companies require complicated passwords. This is a problem because users that do not know the ramifications will re-use passwords on different systems, even if they are told not to. The average user is not concerned for the safety of their own data because they feel that their information is taken care of.

This attitude largely in contrast to the way the early internet was treated by users; users were very afraid of the unknown capabilities of hackers and refused to buy anything online. The psychology of the average user has changed since then, many users are young and do not have the experience of life before the internet.

This is complicated because these companies’ motives are mainly to make money. Companies will only budget what they feel is the minimum amount of money required to make more money. In the security department this would mean keeping users’ data safe enough to stop known hackers but usually not enough to stay ahead of the game. Research costs money and if a company never needs to use these new methods of stopping hackers the research was a waste of money. Many hackers have the same goal, to make as much money as they can, but the attitude toward research is the opposite. The more time a hacker spends researching the more likely they are to be successful.

This is further complicated by the fact that many people do not use unique usernames/passwords for each individual system they. As a result, when one system is hacked the username/password for other systems are compromised. Human psychology is not taken into consideration so, when users do not act the way they are asked to, serious security holes arise. Companies tell their users that their data is safe and users are not educated enough to do anything but believe that these companies are keeping their data safe. Unknowingly to the user the security of their data largely relies on the user him/herself.

In an attempt to keep data private companies require complex passwords and often require users to change passwords often. This leads to using similar passwords over and over so users can remember them. Humans nearly always try to do things the easiest way possible, so their ignorance to the dangers and affinity for laziness are compromising their data on all of the systems they use.

This problem is compounded when social media is taken into account. If a user’s Facebook account is hacked their relatives, friends, likes, and other personal data are visible. This allows a hacker to get data that could help answer security questions elsewhere. For example, a hacker could learn the user’s mother’s maiden name, spouse, children, favorite band, religious views, and so on. With this information a hacker has a higher chance of changing the information on a bank account or transferring funds once s/he has logged in.

This should be studied and demands our attention because hackers understand the ignorant and/or lazy password creating mentality and are constantly taking advantage of the shortcomings of these companies that tell the public that they have everything under control.

The quotes I will be using can be divided into three categories: those that comment on user’s obligation to protect their own data, those that comment on human psychology with respect to technology, and those that have an insight in hacker mentality.

There are many guidelines to making a proper password on the internet. A quick Google search will bring up countless pages that will guide anyone on creating an uncrack-able password.

Many people seem to have an insight into great password creation, but Lorrie Faith Cranor explains an issue with the system entirely. Cranor, according to her bio from her TED talk, “… studies online privacy, usable security, phishing, spam and other research around keeping us safe online …” at Carnegie Mellon University. She advises, “instead of telling people that they need to put all these symbols and numbers and crazy things into their passwords, we might be better off just telling people to have long passwords” (Cranor).

She and her research team were not able to find reliable data on password creation, so they conducted their own rather unique studies on passwords. “The National Institute of Standards and Technology has a set of guidelines which have some rules of thumb for measuring entropy, but they don't have anything too specific, and the reason they only have rules of thumb is it turns out they don't actually have any good data on passwords” (Cranor). Entropy is a measure of how strong a password is.

So Cranor, with her team, set out to get good data on password creation. She began by surveying around campus and got nearly 500 samples. Their university had just required everyone to change their passwords when they adopted a new set of policies. She explains, “ We found that most people knew they were not supposed to write their password down, and only 13 percent of them did, but disturbingly, 80 percent of people said they were reusing their password” (Cranor). One of the most widely seen guidelines from doing a Google search is to make each password unique. This is widely believed to be fundamental to personal online security. Cranor explains, “Now, this is actually more dangerous than writing your password down, because it makes you much more susceptible to attackers.” This is because, once your passwords are known, they can be tried on other systems e.g. a banking site.

Cranor expressed that this was a good start but almost 500 samples is not large enough to reach accurate conclusions for the population at large. They were able to find stolen username/password sets on the internet and began studying them. “… it turns out there are a lot of people going around stealing passwords, and they often go and post these passwords on the Internet.  So we were able to get access to some of these stolen password sets” (Cranor). But these are only a sample of passwords that have been cracked and is not a good sample of the whole; none of the good passwords are represented.

Cranor and her team set out to study this in much more depth. They set up a survey that would pay $0.50 each for two visits. The first visit would require the user to create a login and two days later they could collect another $0.50 cents by logging back in. “…We collected 5,000 passwords, and we gave people a bunch of different policies to create passwords with.” (Cranor). She required different styles of passwords, some with a Basic8 style, where the only requirement was a password of eight characters, while others had a Basic16 requirement. But another portion had a much more complicated requirement, “… it had to have eight characters including uppercase, lowercase, digit, symbol, and pass a dictionary check” (Cranor). There were other requirement groups as well but she did not elaborate.

The findings were illuminating, “we found that the long passwords were actually pretty strong, and the complex passwords were pretty strong too” (Cranor). Complex passwords are very secure but hard to remember, which lends to the re-use of passwords. “When we looked at the survey data, we saw that people were really frustrated by the very complex passwords, and the long passwords were a lot more usable, and in some cases, they were actually even stronger than the complex passwords” (Cranor).

This example shows a unique insight to how people treat their own security. This blasé faire attitude is common among users just learning about the internet. Katie LeClerc Greer, former Direct of Internet Safety for the Massachusetts Attorney General’s Office and Intelligence Analyst for the Massachusetts State Police, says, “I frequently get questions like this: ‘I don’t really know this kid, but my friends are friends with him and he looks my age, so also I friended them on this chat app…is that OK?’” Children are not being taught security by their parents, likely caused by the parent’s lack of knowledge on the subject. “The mere fact that they’re asking this question scares me, and lets me know they really don’t know any better*”* (Greer). There are many threats to a child’s safety when they are not kept hidden on these technologies. “I quickly let them know it’s not OK to communicate with individuals they don’t know personally.  These types of questions are the only proof I need when instructing parents to check their kids’ apps and friend lists often” (Greer). When parents do not know enough about the risks people like Greer have to teach children that it is not permissible to have this kind of contact with unknown people.

Not only personal security is at risk, many businesses do not take proper care of their data. “If you’re not related to the information technology industry, you may think you’re exempt from caring about, or investing in, the latest security technology to protect your company” (Pham). Just as with parents, this is because many business owners do not understand the risks, which is unfortunate because these businesses are not only handling their own data. “Being a brick and mortar store that sells physical tools is no excuse to handle customer data with carelessness” (Pham). Large companies are not immune to this either, there have been many examples of large companies losing data. For instance, in 2014 “Home Depot was … slow to adopt certain security practices, like the latest encryption methods, that of which wasn’t rolled out completely until last week after starting in April, after hackers had already been exfiltrating data for months” (Pham).

The average user used to be afraid to put their information on the internet, but those that have grown up knowing the internet are much more trusting. “five – ten years ago … putting your credit card into a web site to order something was still really sketchy to a lot of people. And now enough people have done it that it’s just the norm” (qtd in Clark). Most people that use internet technologies have at least one source for online shopping now.

Now that the norm is to have personal information in the hands of companies, a shift in how security is implemented is being considered, which would be a shift from antivirus to anti-hacker. Symantec is the company that produces Norton Antivirus (one of the most popular antivirus programs in the world). “Symantec's senior vice president for information security, Brian Dye, told the Wall Street Journal that antivirus ‘is dead.’”(Newman). This is because the company recognizes that hackers will always exist and that they will always be behind if they keep doing things the way they are. “Symantec’s statement, “Antivirus is dead” in May of this year … denotes how outdated their own software is, and its own inability to defend against attackers” (Pham). This shift is largely because systems are getting so large that plugging all of the security holes is difficult. “He is leading Symantec toward a new approach that focuses on spotting hackers within a system and minimizing damage from them instead of trying to keep them out. ‘We don't think of antivirus as a moneymaker in any way.’” (qtd Newman).

Personal security is largely left up to users, but those users do not always know this. There is little data on how well users do their part to keep their own data secure, but the present data from a few small studies shows that there is much room for growth. This is especially important to consider when many companies are losing users’ data to hackers at no fault of the users. There is precedence to study these areas more thoroughly and possibly restructure the current methods of online security.

Works Cited

Clark, Josh. “TechStuff Gets Flushed”. *TechStuff.* March 18, 2015. HowStuffWorks.com. Accessed on April 4, 2015.

Cranor, Lorrie Faith. “What’s wrong with your pa$$word?” TED.com. Web. March 2014. Accessed on March 27, 2015.

Greer, Katie LeClerc. “Ignorance is Dangerous When It Comes to Technology” *iKeepSafe.org.* Web. Oct 2012. Accessed on March 28, 2015.

Griffith, Eric. “Password Protection: How to Create Strong Passwords”. PCMag.com. November 2011. Web. Accessed on March 29, 2015.

Newman, Lily Hay. “Symantec Executive Says Antivirus Is Dead”. *Slate.com*. Web. May 2014. Accessed on April 1, 2015.

Pham, Thu. “A Bad Security Attitude”. *DuoSecurity.com.* Web. September 2014. Accessed on March 28, 2015.