Nathan Brooks

English 2010

Professor Riddle

April 26, 2015

Focus on Basic16 and Two Step Verification For Higher Security

Today’s world requires people to use the Internet multiple times every day. Most people online bank, pay bills, shop, use social media, and have a vast array of other reasons to use the internet. All of these systems require a profile creation along with both a username and password. Most people do not realize the possible dangers to their personal data and end up not following the recommended practices to keep their data safe. Many systems share the same guidelines for creating safe usernames and passwords, but many people bypass any security provided by these guidelines by ignoring them when possible. **Through the comparison of general practices and policies that organizations employ to the results from studies and expert opinion this paper will argue that a Basic16 style of password should be adopted across the board along with adopting a two-step verification method.**

A Basic16 password style is one that requires the user to create a password that is sixteen characters long with no other requirements. Most people are becoming used to the complex passwords that most systems require; they have a set of rules that require the user to add in special characters, numbers, capitals, and sometimes other requirements. A Basic16 password is simpler in every way except that it is longer.

Two step verification is an extra layer of security added on to the standard username/password security. Some users have run into a two-step verification already, but it is not widely adopted; some government web sites require two-step verification. For example, it might make a user answer a security question after giving a name and password, or it could have a code sent to the user’s phone via text that they would have to enter in to the web site to log in. This means that a hacker cannot get through unless they also have the phone that belongs to the compromised user. “2-Step Verification can help keep bad guys out, even if they have your password” (2-Step Verification). It is not hard to deal with an added layer of protection for a user, but it is very difficult for a hacker to get past both layers. They need to know the user’s username and password as usual, but they would also need to be able to answer a specific security question. Traditionally, a common security question might be the user’s childhood dog’s name or the food the user hated when they were growing up.

Almost every person that uses technology has at least one account that has been compromised and been forced to change their passwords. It is scarier than many realize. “When a bad guy steals your password, they could lock you out of your account” (“2-Step Verification”). Being locked out of an account means a user’s password has been changed without the user’s knowledge. When the user attempts to log in to the account in question, they are told they have used the wrong password. A hacker could change the security questions so the user cannot even get the password reset on their own. Users end up having to call the business or organization to prove who they are. “With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account. Most people only have one layer – their password – to protect their account” (“2-Step Verification”). Hackers have an easier job when most people have only one layer of protection.

Large companies have adopted the two-step verification model, but only require the second verification if the activity on the account looks suspicious. “Some of largest adopters of this feature, such as Google, Facebook, Microsoft, Yahoo and Twitter, ask you to verify a log-in through two-step verification only if it looks unusual” (Pegoraro). For some, including Facebook, this means that a cookie is stored on the user’s computer as a temporary pass key. It is only mildly effective as a second layer of protection, but there are stronger versions available. With full two-step verification, “you’ll get a security code to your email, phone, or authenticator app every time you sign in on [a device that isn't trusted](http://go.microsoft.com/fwlink/p/?LinkID=286339)” (“About two-step verification”). This second layer is often optional, it does not have the added security of requiring users to answer a security question or verify that they are the owner of the phone number on file.

Hackers will do everything they can to delay getting caught while they attempt to make as much money as possible through the compromised account for as long as they can. When a hacker gets in s/he can “… go through – or even delete – all of your emails, contacts, photos, etc., pretend to be you and send unwanted or harmful emails to your contacts, use your account to reset the passwords for your other accounts (banking, shopping, etc.)” (“2-Step Verification”). While they have a user’s account held hostage they look for as much personal information as possible to hopefully be able to crack other systems.

If a user’s Facebook account gets hacked the hacker could obtain the user’s mother’s maiden name, date of birth, address, phone number, family relations, likes and dislikes, and many other pieces of data that could help them answer security questions on bank accounts or other sensitive data. A break in at a social media web site might be the ticket in to every other account that person might have.

Hackers like to focus on social media because of this chance at a possible pay-off. The reason this is such a huge pay-off for hackers is because so many people use the same username/password combination for everything, including banking. In a small study done at Carnegie Mellon University “80 percent of people said they were reusing their password” (Cranor). This means that hackers have a good chance of finding out all this information about a user and being successful when they try the same username/password combination at popular banking sites. Cranor explains, “Now, this is actually more dangerous than writing your password down, because it makes you much more susceptible to attackers.” Writing passwords down is frowned upon, but is preferable to using the same passwords on multiple systems. “Between four and 20 characters are the difference makers in whether you're able to access your data, communicate with friends, or make your online purchases. The problem is that passwords should be different everywhere you use them, and that can make it difficult to remember them all” (Griffith). On the internet a user’s information is reachable to anyone that can hack a system, but information that is written down is only visible to a person in close proximity, or a person that might look through personal items to steal.

Two-step verification would allow users to write down a password and keep it in their wallet or purse, as many already do, without the worry of having their account completely lost if someone stole the paper on which they wrote the password. This is because, once the unexpected behavior is noticed on a system, the user could be notified of the strange activity and change their password. This practice would keep bad guys out even if they got ahold of the paper with the credentials.

A third layer of security that is recommended by many companies is a physical dongle that generates a code at login time. Blizzard (the company that produces World of Warcraft) advocates for the use of this added layer of security. “Once linked to your account, the dongle generates a one-time six-digit passcode at the press of button to supplement your regular account password. And because the dongle stays separate from your PC, it's impervious to keyloggers and other similar malware” (Lilly). This is a very different practice from most banks even. “Notably absent from this … are banks and other financial institutions. It’s a shame that you can use two-factor authentication to protect your in-game currency in an MMORPG, but not the real money in your bank account” (Hoffman). For example, during the sign-in process for World of Warcraft, a user that has enabled this security dongle cannot get access to the valued content without it. This means that, if the user’s name and password have been compromised, a hacker can still not gain access to the account. In contrast, many banks only require a username and password to get access to things like fund transferring and bill paying.

Many businesses do not take proper care of their data or their users’ 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). Not many small businesses use a two-step approach to security. Instead they rely only on the standard username/password one-layer version.

Instead of a two layer verification, companies have implemented a higher complexity password requirement. This means that a user has to come up with something that has the special characters, capitals, and/or numbers. A two-step verification is more preferred because, in a one-step system, once a password is stolen it does not matter what the password was in the first place. It can be as complicated as a user wants, but if a hacker gets ahold of it, all is lost.

Companies usually require users to have a complex password. Users that do not know the ramifications will re-use passwords on different systems, even when they are warned 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. Most users do not realize the effect they have on their own security. In an attempt to keep data private companies require complex passwords and often require users to change passwords often. This leads to users using similar passwords over and over because complex passwords are hard to remember.

Humans usually try to do things the easiest way possible, their ignorance to the real dangers and their affinity for laziness are compromising their data on all of the systems they use. This attitude is 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 the early days, many users are young and do not have the experience of life before the internet. They do not have the fear that previous generations.

Companies have attempted to require users to have good security practices by requiring complex passwords, but the laziness and ignorance of the average internet user is overriding this effort. When a user re-uses a password on different systems they jeopardize more than they realize.

A Basic16 password standard could alleviate much of these problems. When added up, some people have a surprisingly high number of username/password combinations that they are expected to remember, never write down, and change often. There is an uncountable number of articles on the internet that give advice as to how one should create the right kind of password. They all have guidelines for trying to make a password that is complicated enough to make cracking it nearly impossible. But these articles mostly all focus on the eight character, numbers, caps, symbols, guideline.

In 2011 PCMag’s Eric Griffith suggested many different methods for creating a solid, random looking password. For example, one of these suggests that it is a good idea to make a password based on a pattern on the keyboard. “A counter-clockwise spin around the letter d could result in ‘rewsxcvf.’ Throw in some random caps and numbers to really lock it down” (Griffith, 2). It is also widely suggested to create passwords by starting a word you can remember and modify it. One could re-write it backwards, replace certain letters with memorable numbers, or swap some similar looking special characters for a letter, just to name a few guidelines. “As long as your replacement makes sense to you, that's all that matters. A ‘^’ for an ‘n’ makes sense to me” (Griffith, 2). These types of guidelines are suggested in a countless number of articles, but hackers are still getting passwords and trying them on multiple systems.

The problem is not the level of entropy a password has (a measure of password strength), the problem lies in the habits of the users. These countless guidelines are a good solution to make one good, strong password. But the number of unique passwords a standard user is supposed to keep in memory far exceeds the number of passwords each person is capable of remembering, especially when passwords are supposed to be changed so frequently.

Many people use only one password for everything and are perfectly fine. They use the same small number of passwords for years on multiple systems. Their sense of security is false, they have security through obscurity. This does not inform them that their password security is too low. It is similar to how a person could speed their entire lives and never be caught by the police, or how many people carry cash on their person and never get mugged. Getting caught is currently the only motivator for a positive change.

The only other manageable way to remember upwards of fifty unique, hard to crack passwords (other than writing them down) is to use a password manager. “If you don't use a strong and unique password for every website, you're asking for trouble. And if you have more passwords than you can count on your fingers, the only way to achieve that goal is by using a password manager” (Rubenking). A password manager is a program that will store all passwords and the user sets a master password to gain access to their small database of stored passwords. The password manager remember passwords so users do not have to, which allows users to make incredibly complex passwords that are encrypted based on the master password. This is good as long as the master password does not fall into the wrong hands. Many internet browsers have password managers as part of their programming, and, depending on the browser, the master password could be stored locally; the user is usually required to be logged in. This is useful but it also means that passwords are being stored locally on a machine where anyone who breaks in can see.

These types of password managers are not ideal because most users leave themselves logged in at all times and do not turn their computers off right after they are done using them. There are many viruses that allow a hacker to gain access to a computer, and a computer that is left on can be manipulated if a hacker has found a back--door

A separate password manager program is preferred because users close the program after they are done using it, which closes any vulnerabilities associated with leaving it open, and because the separate password manager encrypts passwords and will even generate passwords if the user wants it.

Password managers are a good solution for the problem that humans on the internet face. Password managers will remember passwords so users do not have to, but this still means passwords are being written down or stored somewhere. The most ideal would be if humans could remember all of their passwords.

The findings of Lorrie Cranor’s study show that a Basic16 password style would be beneficial, “we found that the long passwords were actually pretty strong, and the complex passwords were pretty strong too”. 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). The push for shorter, more complex passwords might be the wrong way of going about solving problems.

A person can make a Basic16 password based on something they personally remember about a web site and be able to remember it easily. For example, a banking web site’s password could be “ifirstcametothisbankinjune”. Not only is this is extremely easy for someone to remember because it is something personal that cannot be data mined from social media, it is extremely secure. When entered in to HowSecureIsMyPassword.net the result is “It would take a desktop PC about 48 quintillion years to crack”. A super-computer could crack this in about one million years, but hackers do not think this way. Not many of them have access to a super computer, and it would still take too long. They normally try for a while and move onto a different target if they are not successful after a while.

This style of password would remove the need for password manager apps to maintain passwords that are impossible to memorize and would drastically increase internet security. People can easily come up with a small phrase that reminds them of the system they are using that would be memorable.

Users ignore the practice guideline because it is impossible for users to remember so many unique passwords with the current requirements. Through the combination of multiple variations of two step verification and a switch to a Basic16 password schema, users could be un-incentivized to re-use passwords on multiple systems. This would make hacking much harder in general and could make the effort not worth it anymore.

If this topic were studied more thoroughly the findings could be presented to all kinds of business and technology professionals. Businesses could see a drop in costs and their customers would have higher trust. Those that study computer science could be aware of these issues and incorporate better practices in their methods. This issue deserves more attention as it is a large problem that many different organizations have to deal with.

The Basic16 guideline should be adopted and two-step verification should be used whenever possible. Many organizations already use a two-step verification to keep their users’ data safe, but not often enough. The average person is not aware of the dangers of re-using passwords across different systems and they do not have the incentive to follow the safer, less convenient guideline, which is to make unique passwords on every site. The average user also cannot remember so many unique passwords when they have number and symbol requirements. To keep users’ data safe while they online bank, shop, and use social media, a revamp of the status quo is in order.

Works Cited

“2-Step Verification”. *Google.com.* Web. Accessed on April 14, 2015.

“About two-step verification”. *Microsoft.com*. Web. Accessed on April 16, 2015.

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

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

## Hoffman, Chris. “Secure Yourself by Using Two-Step Verification on These 16 Web Services”. *HowToGeek.com*. December 2012. Web. Accessed on April 16, 2015.

“How secure is my password?”. *howsecureismypassword.net.* Web. Accessed on April 19, 2015.

# Lilly, Paul. “Blizzard Offers Additional Layer of Security with Authenticator Dongle”. *MaximumPC.com.* July 2008. Web. Accessed on April 16, 2015.

Pegoraro, Rob. “Two-step verification: It’s a trust issue”. *USAToday.com*. April 2014. Web. Accessed on April 14, 2015.

Rubenking, Niel J. “The Best Password Managers for 2015”. *PCMag.com*. February 18, 2015. Web. Accessed on April 19th, 2015.