Integrating Colors into Passwords to Improve Cyber Security

Author: Elizabeth M. Larson
Mentor: Jeffery R. Wehr
April 18, 2017
Advanced STEM Research Laboratory, Odessa High School, 107 E 4th Avenue, Odessa, WA, 99159
Email: eml2017@yahoo.com
Phone: (509) 982-2111 ext. 214

Key Words:

Cyber security, passwords, encryption, cybercrime

ABSTRACT

Strong passwords (passwords that balance security and memorability) are an effective method of preventing cybercrime. Incorporating the option to add colors into passwords can be a way to do this. The experiment set out to integrate colors into passwords, with at least 30% of tested passwords having a strength greater than 80%. Using an HTML website and a password strength checking website, the top 100 most popular passwords were tested. The HTML website had colored buttons that, when clicked, added a string of characters to the password. The online password meter calculated the password's percentage. Each password was tested with and without the addition of these color codes. The control group (without colors) had an average password percentage of 7.460% (±7.940%) and the experimental group (with colors) had an average password percentage of 99.940% (±0.600%). The hypothesis was accepted, because the addition of colors improved the passwords' percentages. All 100 passwords had a password percentage greater than 80%. With more than one-quarter of the world having access to the Internet, an improved way to make passwords benefits many. It helps keep customer's information secure and helps businesses from losing millions of dollars to cybercrime.

Introduction

The average cost of cybercrime has risen over the past few years, from $7,217,030 in 2013 to $7,721,552 in 2015 [1]. Strong passwords are an effective way to protect businesses from losing copious amounts of money. Websites may require users to follow a "password policy" to create a strong password, one that balances security with memorability (Figure1).

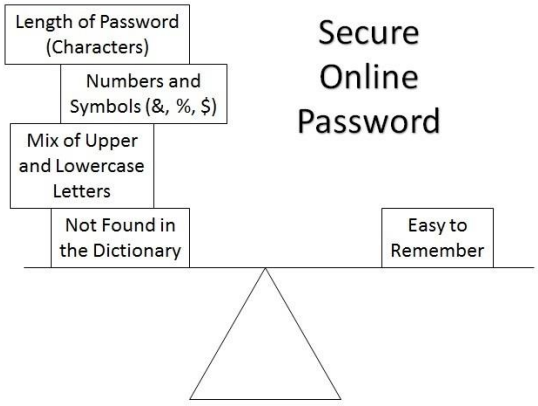


Figure 1: A strong, secure password often includes upper and lowercase letters, numbers, symbols, are lengthy (in terms of number of characters), and cannot be found in the dictionary (to prevent vulnerability to dictionary attacks). Balancing password security and memorability is a difficult task. Passwords must be difficult to guess, but easy to remember.

Password policies of high-profile (social media and email) and high-risk (health, banking, and government) often sacrifice security for memorability. In fact, Facebook, one of the most popular websites on the Internet, only requires a minimum of six characters for a password [2]. A survey conducted by Carnegie Mellon University and Pennsylvania State University further verified this, revealing that security is often compromised for memorability [3]. This could be because system administrators want to avoid losing users over tedious policies. If a password policy is too difficult to follow, the customer will use a different website. A survey conducted by Carnegie Mellon University found that 31% of users will physically write out their password, thus indicating that the majority of users rely on remembering the password. This study also concluded that a 16-character minimum with no additional numbers of symbols is considered both strong and user-friendly [4]. However, there is a flaw in this policy; a password that is the letter “a” typed 16 times is easier to decipher than a string of words that result in one long 16-letter password, such as, “strongerpassword”.

Incorporating other credentials, such as colors, to these password policies may serve as a solution. Psychological studies have revealed that it is easier for the human brain to remember visual information that textual information [5, 6]. Because of this, integrating the option to add colors to a password policies allows the user to have a complex, yet memorable, password. For example, the susceptible and globally used password, “password” will be harder to decipher if combined with colors (Figure 2).

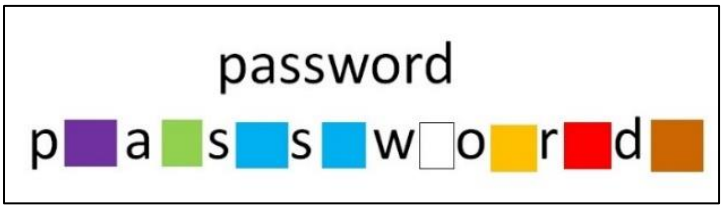


Figure 2: “password” is one of the most popular passwords. Its simplicity makes it easy to remember, but also vulnerable to hackers. Adding colors behind each letter makes the password more difficult to figure out, without sacrificing its memorability. In the figure, for example, using the color purple after “p” will be easy to remember, because “purple” begins with the letter “p”.

The experiment set out to integrate colors into passwords, with at least 30% of tested passwords having a strength greater than 80%. While the task of balancing security with usability is difficult, the results outweigh the risks. The new policy appeals to users of all skill levels, and was more secure than policies already used online [7, 8]. With more than one-quarter of the world having access to the Internet, an improved password policy has a profound global effect [9]. Also, approximately 90% of Internet users own and use email accounts, which can hold personal information [10]. Combining colors with the traditional password will make these accounts more secure, while still being easy to memorize.

Each person associates colors and letters differently. One person may associate the color blue with the letter “s”, because the sky is blue. However, another person may associate the color green with the letter “s”, because snakes are green. Integrating colors into passwords allows each

password to be individual to the user, and therefore easier to memorize. Also, it is very difficult for a computer or hacker to guess each color. This lessens the likelihood of the password being cracked. Personal information is safer, and the user will not forget the password.

Materials and Methods

A system for testing the strength of the passwords with and without the addition of colors was established. A short HTML form was coded. The form allowed the user to enter their passwords using the keys on their keyboard and the colored buttons displayed on the screen. The user also had the option of hiding and showing their password. Clicking the colored buttons inserted a string of characters into the password. Red was Ftn%uRRg2q, green was Jak6jo^wQE, blue was pEUbCA#2NV, cyan was hu$r9RBnkG, magenta was fHvknD#0CK, yellow was e@2dCMfaOL, and black was PkuFVr!nO6. These color codes were created using a website that randomized letters and numbers [11]. One symbol was also added to each code, to confirm that all the components of a strong password were included (Figure 3-4).

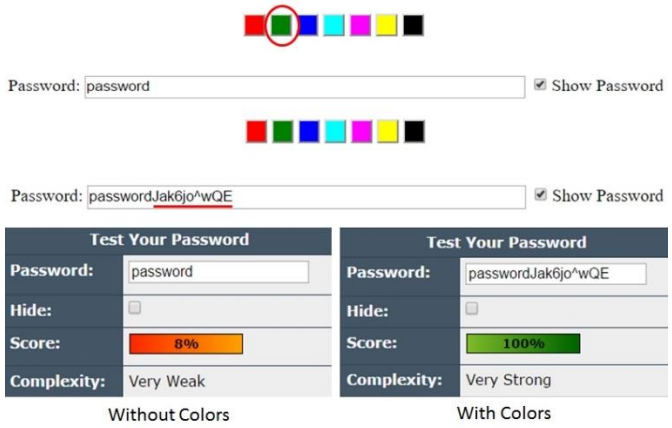
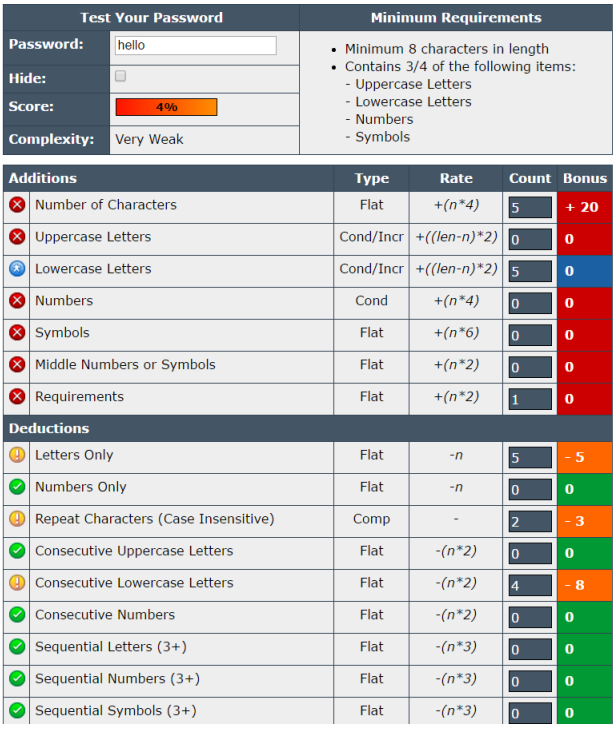


Figure 3: When the colored buttons were clicked, the color's code appeared in the input box. In the experiment, cyan's color code was Jak6jo^wQE. "password" without the color code was given an 8% password percentage, whereas "password" with the color code was given 100%. Essentially, the codes made each password longer (in characters) and more complex, and all the user needs to remember was "password cyan".

```
<html>
<head>
<title>Create a Password</title>
</head>
<body>

<form name="calculator" >
<center>
<input type="button" style="background-color:#FF0000;width:20px" onClick="document.calculator.ans.value+='Ftn%uRRg2q'">
<input type="button" style="background-color:#008000;width:20px" onClick="document.calculator.ans.value+='Jak6jo^wQE'">
<input type="button" style="background-color:#0000FF;width:20px" onClick="document.calculator.ans.value+='pEUbCA#2NV'">
<input type="button" style="background-color:#00FFFF;width:20px" onClick="document.calculator.ans.value+='hu$r9RBnkG'">
<input type="button" style="background-color:#FF00FF;width:20px" onClick="document.calculator.ans.value+='fHvknD#0CK'">
<input type="button" style="background-color:#FFFF00;width:20px" onClick="document.calculator.ans.value+='e@2dCMfaOL'">
<input type="button" style="background-color:#000000;width:20px" onClick="document.calculator.ans.value+='PkuFVr!nO6'">

<br><br><br>Password: <input type="password" name="ans" style="width:400px;" id="password">
<input type="checkbox" onchange="document.getElementById('password').type = this.checked ? 'text' : 'password'">Show Password

</form>
</body>
</html>
```

Figure 4: The HTML code used to add colors to a password. This method of color code addition was similar to an online calculator. When the user clicks on the colored buttons, the string of characters appears in an input box.

To test the strength of each password, The Password Meter was used. This website used a series of equations to calculate the password percentage. Rather than determining the "time-to-crack" of the passwords, the equations used the components of the password to calculate an overall percentage. The password percentage was larger if the password included uppercase letters, lowercase letters, numbers, symbols, middle numbers or symbols, and/or met the website's requirements of an 8-character minimum. Also, each character in the password added 4% to the overall score. Deductions included passwords was comprised of only letters, only numbers, repeated characters, consecutive uppercase letters, consecutive lowercase letters, consecutive numbers, sequential letters, sequential numbers, or sequential symbols (Figure 5) [12].



Test Your Password		Minimum Requirements
Password:	hello	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	4%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	5	+ 20
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	1	0
Deductions				
Letters Only	Flat	-n	5	- 5
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 3
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Figure 5: The Password Meter website followed a series of equations to find each password percentage. As seen in the figure, the password “hello” received a score of 4%. The five characters were multiplied by four, resulting in a 20% password percentage. However, the password was only letters (5% was taken off), characters were repeated (3% was taken off), and there were four consecutive lowercase letters (these four multiplied by two resulted in 8% being taken off the total score). In the rate column, n refers to the total number of occurrences and len refers to the total password length.

One hundred passwords were tested using The Password Meter. These passwords came from a website that listed the 10 million most popular passwords [13]. The password percentages were recorded as the control group. These 100 passwords were then tested with the addition of one color code. Each color code was 82% on their own. The passwords with colors were then entered into a website that calculated the password percentage. This group of passwords were recorded as the experimental group. The control and experimental group were statistically analyzed using a two-tailed t-test.

Results

The control group, the passwords without the addition of color codes, had an average password percentage of 7.460% (±7.900%). The experimental group, the passwords with the addition of colors, had an average password percentage of 99.940% (±0.600%). The Password Meter also displayed a visual representation of the password complexity. The site determined if the password was very weak, weak, good, strong, or very strong. This was also recorded in the data table (Table 1).

Password (Control Group)	Control Percentage	Control Complexity	Password with Colors (Experimental Group)	Experimental Percentage	Experimental Complexity
123456	4%	Very Weak	123456Ftn%uRRg2q	100%	Very Strong
password	8%	Very Weak	passwordJak6jo^wQE	100%	Very Strong
12345678	4%	Very Weak	12345678pEUbCA#2NV	100%	Very Strong
qwerty	8%	Very Weak	qwertyhu$r9RBnkG	100%	Very Strong
123456789	4%	Very Weak	123456789fHvknD#0CK	100%	Very Strong
12345	4%	Very Weak	12345e@2dCMfaOL	100%	Very Strong
1234	4%	Very Weak	1234PkuFVr!nO6	100%	Very Strong
111111	0%	Very Weak	111111Ftn%uRRg2q	100%	Very Strong
1234567	4%	Very Weak	1234567Jak6jo^wQE	100%	Very Strong
dragon	8%	Very Weak	dragonpEUbCA#2NV	100%	Very Strong
123123	7%	Very Weak	123123hu$r9RBnkG	100%	Very Strong
baseball	4%	Very Weak	baseballfHvknD#0CK	100%	Very Strong
abc123	32%	Weak	abc123e@2dCMfaOL	100%	Very Strong
football	7%	Very Weak	footballPkuFVr!nO6	100%	Very Strong
monkey	8%	Very Weak	monkeyFtn%uRRg2q	100%	Very Strong
bball	0%	Very Weak	bballJak6jo^wQE	100%	Very Strong
shadow	8%	Very Weak	shadowpEUbCA#2NV	100%	Very Strong
master	8%	Very Weak	masterhu$r9RBnkG	100%	Very Strong
3333333	0%	Very Weak	3333333fHvknD#0CK	100%	Very Strong
qwertyuiop	12%	Very Weak	qwertyuiope@2dCMfaOL	100%	Very Strong
123321	4%	Very Weak	123321PkuFVr!nO6	100%	Very Strong
mustang	9%	Very Weak	mustangFtn%uRRg2q	100%	Very Strong
1234567890	7%	Very Weak	1234567890Jak6jo^wQE	100%	Very Strong
michael	9%	Very Weak	michaelpEUbCA#2NV	100%	Very Strong

654321	4%	Very Weak	654321hu$r9RBnkG	100%	Very Strong
8888888	0%	Very Weak	8888888fHvknD#0CK	100%	Very Strong
superman	10%	Very Weak	supermane@2dCMfaOL	100%	Very Strong
1qaz2wsx	38%	Weak	1qaz2wsxPkuFVr!nO6	100%	Very Strong
7777777	0%	Very Weak	7777777Ftn%uRRg2q	100%	Very Strong
6666666	0%	Very Weak	6666666Jak6jo^wQE	100%	Very Strong
121212	1%	Very Weak	121212pEUbCA#2NV	100%	Very Strong
0	3%	Very Weak	0hu$r9RBnkG	94%	Very Strong
qazwsx	8%	Very Weak	qazwsxfHvknD#0CK	100%	Very Strong
123qwe	35%	Weak	123qwee@2dCMfaOL	100%	Very Strong
2016	10%	Very Weak	2016PkuFVr!nO6	100%	Very Strong
2015	10%	Very Weak	2015Ftn%uRRg2q	100%	Very Strong
jordan	8%	Very Weak	jordanJak6jo^wQE	100%	Very Strong
jennifer	9%	Very Weak	jenniferpEUbCA#2NV	100%	Very Strong
zxcvbnm	9%	Very Weak	zxcvbnmhu$r9RBnkG	100%	Very Strong
asdfgh	5%	Very Weak	asdfghfHvknD#0CK	100%	Very Strong
hunter	8%	Very Weak	huntere@2dCMfaOL	100%	Very Strong
buster	8%	Very Weak	busterPkuFVr!nO6	100%	Very Strong
soccer	6%	Very Weak	soccerFtn%uRRg2q	100%	Very Strong
harley	8%	Very Weak	harleyJak6jo^wQE	100%	Very Strong
batman	7%	Very Weak	batmanpEUbCA#2NV	100%	Very Strong
andrew	8%	Very Weak	andrewhu$r9RBnkG	100%	Very Strong
tigger	6%	Very Weak	tiggerfHvknD#0CK	100%	Very Strong
sunshine	9%	Very Weak	sunshinee@2dCMfaOL	100%	Very Strong
iloveyou	9%	Very Weak	iloveyouPkuFVr!nO6	100%	Very Strong
qwertyuiop	12%	Very Weak	qwertyuiopFtn%uRRg2q	100%	Very Strong
2000	0%	Very Weak	2000Jak6jo^wQE	100%	Very Strong
charlie	9%	Very Weak	charliepEUbCA#2NV	100%	Very Strong
robert	7%	Very Weak	roberthu$r9RBnkG	100%	Very Strong
thomas	8%	Very Weak	thomasfHvknD#0CK	100%	Very Strong
hockey	8%	Very Weak	hockeye@2dCMfaOL	100%	Very Strong
ranger	7%	Very Weak	rangerPkuFVr!nO6	100%	Very Strong
daniel	8%	Very Weak	danielFtn%uRRg2q	100%	Very Strong
starwars	8%	Very Weak	starwarsJak6jo^wQE	100%	Very Strong
klaster	9%	Very Weak	klasterpEUbCA#2NV	100%	Very Strong
112233	0%	Very Weak	112233hu$r9RBnkG	100%	Very Strong
george	6%	Very Weak	georgefHvknD#0CK	100%	Very Strong

1111111	0%	Very Weak	1111111e@2dCMfaOL	100%	Very Strong
computer	10%	Very Weak	computerPkuFVr!nO6	100%	Very Strong
michelle	8%	Very Weak	michelleFtn%uRRg2q	100%	Very Strong
jessica	7%	Very Weak	jessicaJak6jo^wQE	100%	Very Strong
pepper	0%	Very Weak	pepperpEUbCA#2NV	100%	Very Strong
1111	0%	Very Weak	1111hu$r9RBnkG	100%	Very Strong
zxcvbn	8%	Very Weak	zxcvbnfHvknD#0CK	100%	Very Strong
555555	0%	Very Weak	555555e@2dCMfaOL	100%	Very Strong
11111111	0%	Very Weak	11111111PkuFVr!nO6	100%	Very Strong
131313	1%	Very Weak	131313Ftn%uRRg2q	100%	Very Strong
freedom	7%	Very Weak	freedomJak6jo^wQE	100%	Very Strong
777777	0%	Very Weak	777777pEUbCA#2NV	100%	Very Strong
pass	3%	Very Weak	passhu$r9RBnkG	100%	Very Strong
asdfghjkl	4%	Very Weak	asdfghjklfHvknD#0CK	100%	Very Strong
maggie	6%	Very Weak	maggiee@2dCMfaOL	100%	Very Strong
159753	15%	Very Weak	159753PkuFVr!nO6	100%	Very Strong
aaaaaa	0%	Very Weak	aaaaaaFtn%uRRg2q	100%	Very Strong
ginger	7%	Very Weak	gingerJak6jo^wQE	100%	Very Strong
princess	8%	Very Weak	princesspEUbCA#2NV	100%	Very Strong
joshua	8%	Very Weak	joshuahu$r9RBnkG	100%	Very Strong
cheese	5%	Very Weak	cheesefHvknD#0CK	100%	Very Strong
amanda	6%	Very Weak	amandae@2dCMfaOL	100%	Very Strong
summer	6%	Very Weak	summerPkuFVr!nO6	100%	Very Strong
love	6%	Very Weak	loveFtn%uRRg2q	100%	Very Strong
ashley	8%	Very Weak	ashleyJak6jo^wQE	100%	Very Strong
password1	26%	Weak	password1pEUbCA#2NV	100%	Very Strong
nicole	8%	Very Weak	nicolehu$r9RBnkG	100%	Very Strong
chelsea	8%	Very Weak	chelseafHvknD#0CK	100%	Very Strong
hello	4%	Very Weak	helloe@2dCMfaOL	100%	Very Strong
matthew	7%	Very Weak	matthewPkuFVr!nO6	100%	Very Strong
access	3%	Very Weak	accessFtn%uRRg2q	100%	Very Strong
yankees	7%	Very Weak	yankeesJak6jo^wQE	100%	Very Strong
987654321	4%	Very Weak	987645321pEUbCA#2NV	100%	Very Strong
dallas	5%	Very Weak	dallashu$r9RBnkG	100%	Very Strong
austin	8%	Very Weak	austinfHvknD#0CK	100%	Very Strong
thunder	9%	Very Weak	thundere@2dCMfaOL	100%	Very Strong
taylor	8%	Very Weak	taylorPkuFVr!nO6	100%	Very Strong

matrix	8%	Very Weak	matrixFtn%uRRg2q	100%	Very Strong
Password1	54%	Good	Password1Jak6jo^wQE	100%	Very Strong
Average Password Percentage (Control)	7.460%		**Average Password Percentage (Control)**	99.940%	
Standard Deviation	±7.900%		**Standard Deviation**	±0.600%	

Table 1: The average password percentage without color codes added (controlled group) was 7.460%, with a standard deviation of ±7.900%. The average password percentage with color codes added (experimental group) was 99.940%, with a standard deviation of ±0.600%.

Discussion

The goal of the experiment was to integrate colors into passwords, with at least 30% of tested passwords having a strength greater than 80%. This goal was met; every password in the experimental group was greater than 80%, with 99 passwords at 100% and one password at 94%. There was no overlap of standard deviation between the control and experimental group (Figure 6).

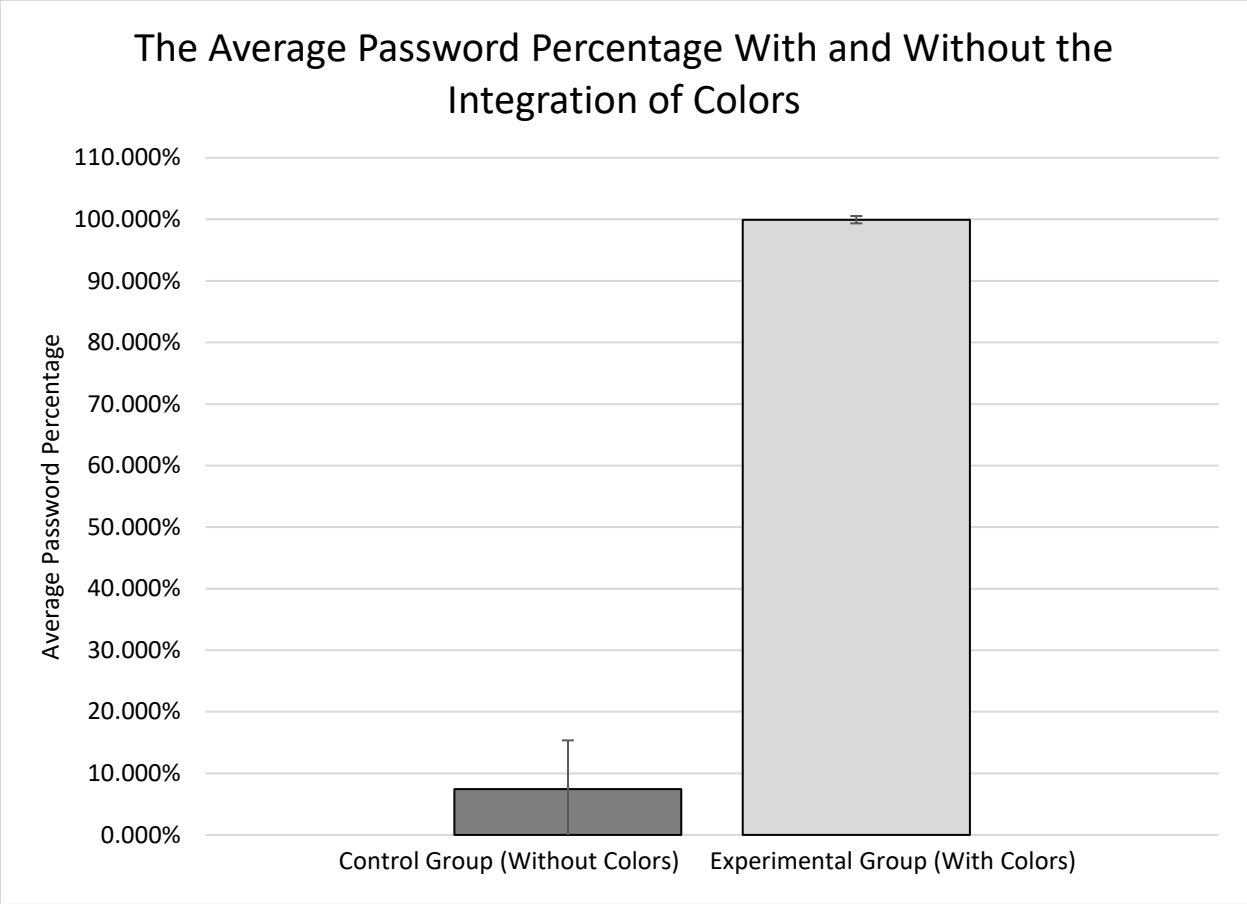


Figure 6: The average password percentage without color codes (controlled group) was 7.000% (±7.900%). The average password percentage with color codes (controlled group) was 100.000% (±0.600%).

After statistical analysis, it was revealed that passwords with added color codes had a higher password percentage than those without color codes. Tests conducted on the password with and without colors were compared using a two-tailed t-test. The average password percentage of with and without the addition of colors was found to be significantly different at the 99.9% confidence level ($t=\pm117.349$, $0.001>p$, $df=198$) (Table 2).

	Control (Without Colors	*Experimental (With Colors)*
Mean	7.460%	99.940%
Standard Deviation	±7.9000%	±0.600%
Observations	100	100
df	198	
P(T<=t) two-tail	5.686 E-185	
t Value two-tail	±3.340	

Table 2: The average password percentage for the control and experimental group were statistically compared using a two-tailed t-test. The control and experimental group were statistically different at the 99.9% confidence level (t=±117.349, 0.001>p, df=198).

In conclusion, the research was a success; the hypothesis was accepted because the addition of colors improved the passwords' percentage. Adding only one color to a password greatly increased the password percentage. With the current password creation process, users can add random strings of characters, similar to the colors codes, to their password. However, doing so implies that the user has the color code memorized. By using the colored buttons to add codes to the password, as opposed to memorizing them, the user only has to remember where each color is. It is easier to remember that magenta comes after the letter "m" than it would be to memorize "mfHvknD#0CK". Colors used in passwords does not need to be limited to the seven used in the experiment. If the experiment were to be continued, the number of colored buttons can increase. Upwards of 10, 20, or even 50 different colors can be added, as long as the number of color options does not overwhelm the user. Further expansion upon these results could be an app that the user downloads and uses anytime they need to create a password. This method uses dual authentication and prevents the tedious process of integrating the "color password" system into every website. High-profile and high-risk websites can use colors to improve password security and memorably amongst customers.

References

1. Ponemon Institute LLC. *2015 Cost of Cyber Crime Study: Global*. 2015. http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

2. Joanne Kuzma. "Account Creation Security of Social Network Sites." *International Journal of Applied Science and Technology* 1, no. 3 (June 2011): 8-13.

3. Ur, Blase, et al. "Do Users' Perceptions of Password Security Match Reality?" *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems – CHI '16* 2016. doi:10.1145/2858036.2858546.

4. Komanduri, Saranga, et al. "Of Passwords and People: Measuring the Effect of Password-Composition Policies." *Proceedings of the 2011 annual conference on human factors in computing systems – CHI '11* 2011: 2601-2. doi:10.1145/1978942.1979321.

5. Paivio, Allan, Timothy Rogers, and Padric Smythe. "Why Are Pictures Easier to Recall Than Words?" *Psychonomioc Science* 11, no. 4 (1968): 137-138.

6. Kirkpatrick, Edwin. "An Experimental Study of Memory." *Psychological Review* 1, no. 6 (November 1894): 602.

7. de Carné de Carnavalet, Xavier and Mohammad Mannan. "From Very Weak to Very Strong: Analyzing Password-Strength Meters." *Proceedings 2014 Network and Distributed System Security Symposium* 2014, 15-18. doi:10.14722/ndss.2014.23268.

8. Klein, Daniel. "'Foiling the cracker': A survey of, and improvements to, password security." *Proceedings of the USENIX UNIX Security Workshop*, (August 1990): pp.5-14.

9. Warf, Barney. "Geographies of Global Internet Censorship." *GeoJournal* 76, no. 1 (November 23, 2010): 1-23. doi:10.1007/s10708-010-9393-3.

10. Nie, Norman and Lutz Erbring. "Internet and Society." *Stanford Institute for the Quantitative Study of Society* 3 (2009): 14-19.

11. Haahr, Mads. "RANDOM.ORG - String Generator". *Random.org*. N.p., 2017. Web. 21 Feb. 2017.

12. Todnem, Jeff. "Password Strength Checker". *Passwordmeter.com*. Web. 13 Jan. 2017.

13. Danielmiessler/Seclists". *GitHub*. N.p., 2017. Web. 3 Feb. 2017.