

# Bachelor of Software Engineering

## Research Analysis

Mobile App UX

CS104.1

LastPass App

# Table of Contents

Objective & Strategy .....	4
Target App.....	4
Discussion with the client .....	4
Business needs:.....	4
User needs: .....	4
Assumptions.....	5
Target Audience .....	6
Target Audience Survey .....	6
Target Audience Research .....	8
Primary Target Audience .....	9
Secondary Target Audience .....	9
Personas.....	9
Mobile UX Research.....	11
SWOT Analysis .....	11
LastPass.....	11
1Password.....	12
RoboForm .....	14
Microsoft Authenticator .....	15
UI elements.....	16
Color Theory.....	17
RGB vs CMYK.....	17
Color wheel .....	18
Color Schemes .....	19
Color Psychology.....	19
Inspiration .....	20
User Testing Research.....	21
Ethics.....	21
Tasks.....	22
Observations Recorded.....	22
Interview Questions.....	22
Results.....	23
Limitations of testers .....	27

Data Analysis .....	27
Graphs .....	27
Card Sorting .....	29
Assumptions Revisited .....	31
Conclusion .....	33
Final App Needs .....	33
Final Plan .....	34
Timeline .....	35
<b>References .....</b>	<b>38</b>

# Objective & Strategy

## Target App

The mobile app we are conducting UX research on is LastPass. A password manager/vault.

Client: LastPass – <https://www.lastpass.com/>

## Discussion with the client

The client wants an app that allows its users to store passwords/logins for accounts. Passwords can be from different accounts. I.e., Gmail, yahoo, Facebook. So the client would like the app to be able to integrate with other apps. An autofill function is what they were referring to. They want the users' passwords/logins to be stored securely. Client needs the app to encrypt their data and only decrypted within the app itself when needed. Also, the ability for the users to go on another device and be able to access their data(passwords/logins). As the app will be dealing with sensitive data the client would like the app data to only be visible to the users. This means that the client cannot and should not be able to see the encrypted document as it will be stored locally to where the user has specified. This ensures the users' privacy.

## Business needs:

- "People's privacy always comes first" – user privacy.
- Maintain reputation.
- Remain secure.
- Provide a password manager tool to users.
- Safely store data. (Encryption and Decryption)

## User needs:

- Secure to use – require the user's password to use.
- Fast/Responsive to use.
- Straightforward process to read/copy usernames/passwords.
- Straightforward process to create/edit logins.
- Easy to navigate through the app.
- Store multiple passwords for different accounts.

# Assumptions

## **Security and Privacy:**

We assume that users think that the platform is secure and dependable to store and access their data. We assume users believe their data is safe within this app as it will have security features, including advanced encryption and/or multi-factor authentication, to ensure that users' data is protected from unauthorized access. As the app being researched is designed to store sensitive information, it is crucial we focus on security and privacy.

We assume that users don't want their passwords being shared - as this would allow other people to login to that user's account. From this assumption we know that the app we are making will need to be secure so that only the user can access their data and no other users who it doesn't belong to.

## **Ease of Use:**

We assume users want to access their passwords as fast as possible while maintaining the security factor. We assume users know how to copy and paste their passwords on their mobile device. We want to make the UI/UX as easy/straight forward as possible to help users access their passwords when needed.

We assume users will need to import or create a username/password for every one of their existing accounts when first using the app, because of this we believe that it is important to make the creation/editing of usernames/passwords as simple and straightforward as possible to make it a less tedious task than it must be.

## **Compatibility:**

We assume users will be working on various platforms and diverse types of mobile devices from Android phone, Apple iPhone, Windows phone and/or Google phone. From this assumption we need to make sure that we account for different devices as we can and make it compatible with them, so the mobile app works the same on every device as expected.

We assume using users will be using a touch screen on their device, so we will need to take this into account when designing the UX/UI for the mobile app as there are multiple factors that can make it hard to use a touch screen including but not limited to small buttons and inconsistent UI.

We assume most mobile devices are handheld and/or fit in a pocket. This means that text size and contrast is going to be important for the user to read on the mobile device easily.

# Target Audience

## Target Audience Survey

To get a reliable insight to our target audience, we sent out a survey to an anonymous forum for people around the world to fill out. The survey results are just an indication of our target audience but helped us reliably define our primary and secondary target audience.

<https://forms.gle/4ghPz4tP9oG9p81u7> - Survey

### Questions:

Price of your current password manager per month: \*

- ☐ Free
- ☐ \$0 - \$5
- ☐ \$5 - \$10
- ☐ \$10+

What is your age (years)

- ☐ Less than 16
- ☐ 16 - 18
- ☐ 19 - 21
- ☐ 22 - 30
- ☐ 31 - 40
- ☐ 40 - 50
- ☐ 50+

Do you feel like your passwords and accounts are safe? \*

- ☐ Yes
- ☐ No
- ☐ Maybe
- ☐ Other: \_\_\_\_\_

How often do you use a password manager? \*

- ☐ Frequently everyday
- ☐ A few times a day
- ☐ About once a day
- ☐ About once a every few days
- ☐ About once a week
- ☐ Almost never

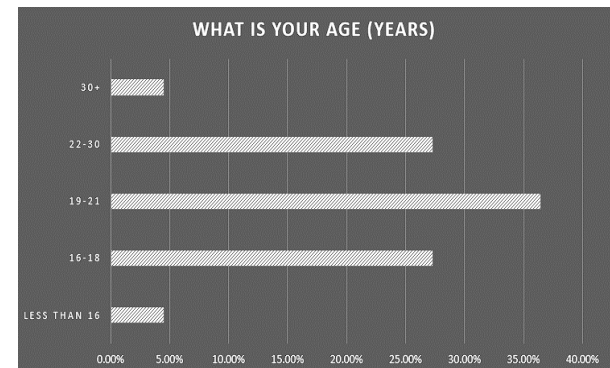
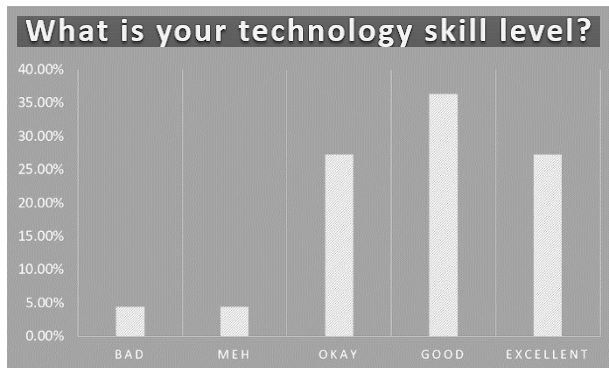
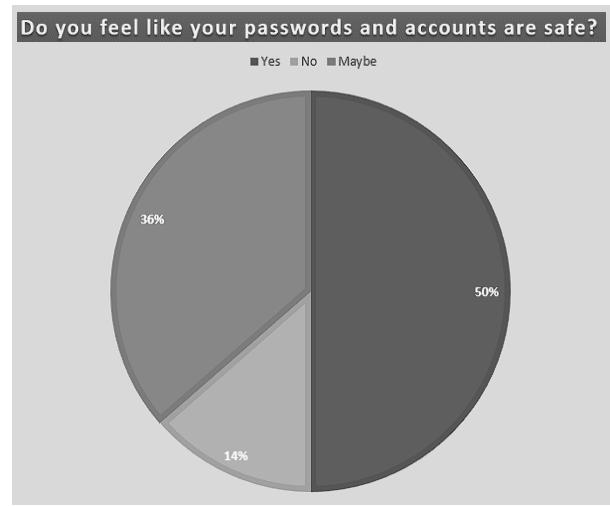
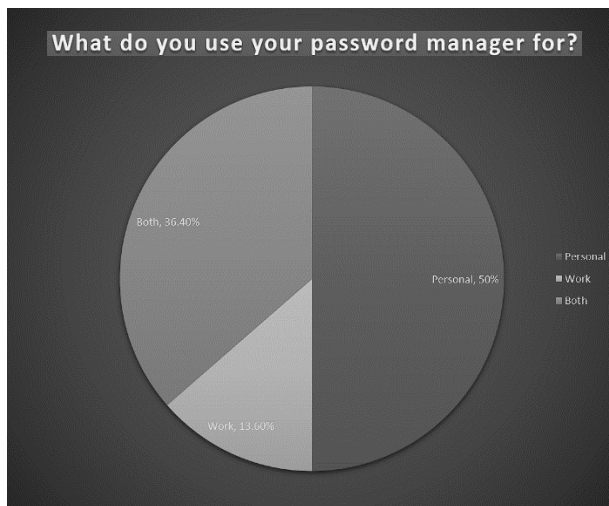
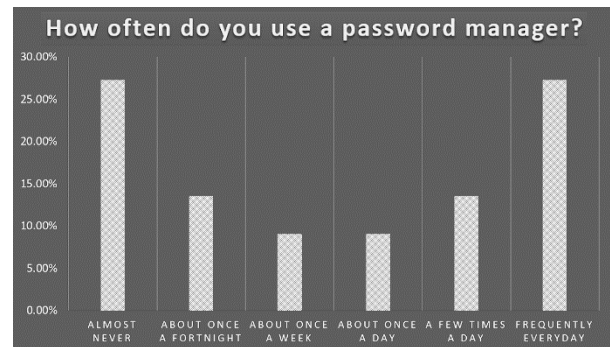
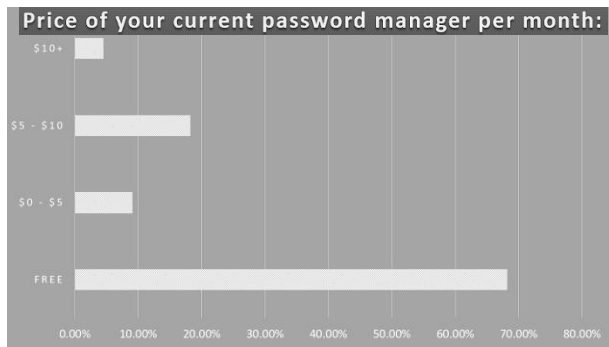
What is your technology skill level? \*

- ☐ 1 - Bad (I have to get help)
- ☐ 2 - Meh (There are some things I will get help with)
- ☐ 3 - Okay (I know how to use technology)
- ☐ 4 - Good (I try help others if they get stuck)
- ☐ 5 - Excellent (Your friends and family seek you out for help)

What do you use your password manager for? \*

- ☐ Work
- ☐ Personal

## Results:

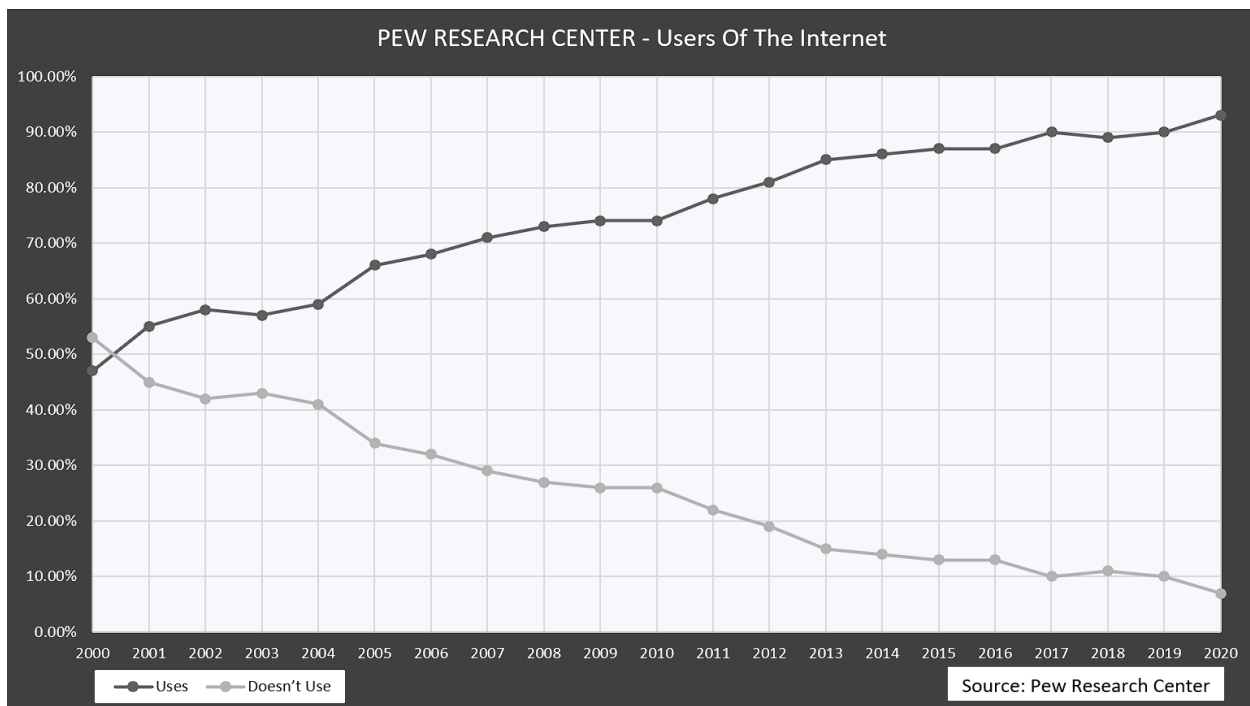


## Target Audience Research

Ivana Vojinovic shared their password statistics and report on 'DataProt' and from these statistics we can make inferences into our target audience. The article says "51% of people use the same passwords for both work and personal accounts." – although this is a different question to our work and personal use for a password manager, we can still infer that our target audience will include work and/or personal use. The article also says, "Only 18% of respondents say that using a password manager is required by their employer." – From this we imply that work related password managers are less used than personal use. From our research and from DataProt's data, we will focus our target audience on two categories: Personal Use and Work Use.

The report on DataProt also says "29% of internet users have more password-protected accounts than they can keep track of." – This shows us one of the problems users have, which our app helps solve this problem. Our password manager LastPass is based on managing users' passwords securely for them so we will keep our focus on the problem it is meant to solve for users.

A trend shown by the Pew Research Center shows that people are in an increasing trend of using the internet. Below is their data put into a chart to put this into perspective from 2000 -> 2020.



This trend shows how general society has developed over time and infers that people of all ages today are more likely to use technology today. This will help us refine our target audience further by implying that younger age groups are more likely to be competent with technology. This trend of technology use and skill is reinforced by our survey data shown earlier.





## Primary Target Audience


Our primary target audience will be young adults aged 18 to 25 of all genders, based on our surveys and research. They would have a medium to elevated level of IT skill level as the younger generation are typically more competent with technology. The target audience will have multiple different online accounts. Occupation is not targeted for the primary target audience as it is focused on personal use. There is no specific region / country as the target audience as the product is worldwide.


## Secondary Target Audience

Our secondary target audience will be adults aged 20+ where their work requires them to have a secure password which is too complicated to remember. This target audience will typically be working for an IT company which requires them to have a secure login. There is no specific region / country as the target audience as the product is worldwide. These could be individuals who work in cybersecurity or government agencies where their login details are highly confidential as they are dealing with sensitive information.

## Personas

	<b>Personal Details</b> <ul style="list-style-type: none"> <li><b>Home</b> Living at home with parents</li> <li><b>Hobbies</b> Beer Pong, Math</li> <li><b>Device</b> Galaxy S10</li> </ul>	<b>Tech Exposure</b> 
	<b>About</b> <p>Nathan is current studying Accounting at Otago University. He has a very logical mind with a strong routine every week. He works for NZ Law as an Accountant which he is very grateful for. Nathan takes his work very seriously but also knows how to let loose because on the weekends he can PARTY!</p>	
<b>Nathan Smith</b> <b>24</b> <b>Part-Time Student &amp; Accountant for NZ Law</b>  <b>QUOTE</b> <i>"I am a very busy person during the week but love going for drink when I can"</i>	<b>Behavior's &amp; Pain Points</b> <ul style="list-style-type: none"> <li>Is not very creative and uses weak passwords.</li> <li>Writes passwords down in notepad on his phone</li> <li>Is quick to get frustrated at slow technology / programs</li> </ul>	<b>Goals</b> <ul style="list-style-type: none"> <li>Wants to graduate university</li> <li>Wants to secure his online footprint</li> <li>Wants to but his own house</li> <li>Wants to spend more time on what matters</li> </ul>

 <p><b>Tabitha Logram</b> 23 Full-Time Art Student</p> <p><b>QUOTE</b> "Drawing is the best way to express my creativity"</p>	<p><b>Personal Details</b></p> <p><b>Home</b> Flatting with friends</p> <p><b>Hobbies</b> Painting, Playing Violin</p> <p><b>Device</b> Apple iPhone XR</p>	<p><b>Tech Exposure</b></p> <p>Low Medium High</p>
	<p><b>About</b></p> <p>Tabitha is currently pursuing her degree in Fine Arts at Victoria University. She has a strong sense of creativity and has a keen eye for detail. Tabitha often uses various online platforms to support her schoolwork. An app that can store and manage her numerous login details, keep her personal information secure and help her simplify her online experience</p>	
	<p><b>Behavior's &amp; Pain Points</b></p> <ul style="list-style-type: none"> <li>• Very creative and free thinking</li> <li>• Open to new ways of creating art</li> <li>• Calm and collected demeanor</li> </ul>	<p><b>Goals</b></p> <ul style="list-style-type: none"> <li>• Wants to recognized as an artist</li> <li>• Wants to have art displayed at Museums</li> <li>• Wants to teach young children painting</li> </ul>

 <p><b>Jarrod Lofar</b> 30 IT Systems Engineer at Window Cleaning Contractors</p> <p><b>QUOTE</b> "No mom I CANT fix your computer..."</p>	<p><b>Personal Details</b></p> <p><b>Home</b> Living in a caravan</p> <p><b>Hobbies</b> Coding, reading tech mags</p> <p><b>Device</b> Galaxy S20</p>	<p><b>Tech Exposure</b></p> <p>Low Medium High</p>
	<p><b>About</b></p> <p>Jarrod looks after the IT infrastructure at Window Cleaning Contractors. Working in the IT industry he has developed a deep understanding of the needs for his company. On a regular basis Jarrod deal with sensitive information, this may include login details, client data and company documents. This means that he requires a secure and effective of storing and retrieving this information. Therefore, Jarrod is looking for an app that combines both high security and ease of retrieving stored data. This will enable him to access and manage data efficiently.</p>	
	<p><b>Behavior's &amp; Pain Points</b></p> <ul style="list-style-type: none"> <li>• Very technical minded and logical.</li> <li>• Keen on learning new Technologies</li> <li>• Prefers quality over quantity.</li> </ul>	<p><b>Goals</b></p> <ul style="list-style-type: none"> <li>• Wants to improve the IT system at his current work</li> <li>• Learn new IT technologies</li> <li>• Teach his company to be more efficient in IT production</li> </ul>

# Mobile UX Research

## SWOT Analysis

Target App – LastPass

Competitor 1 – 1Password

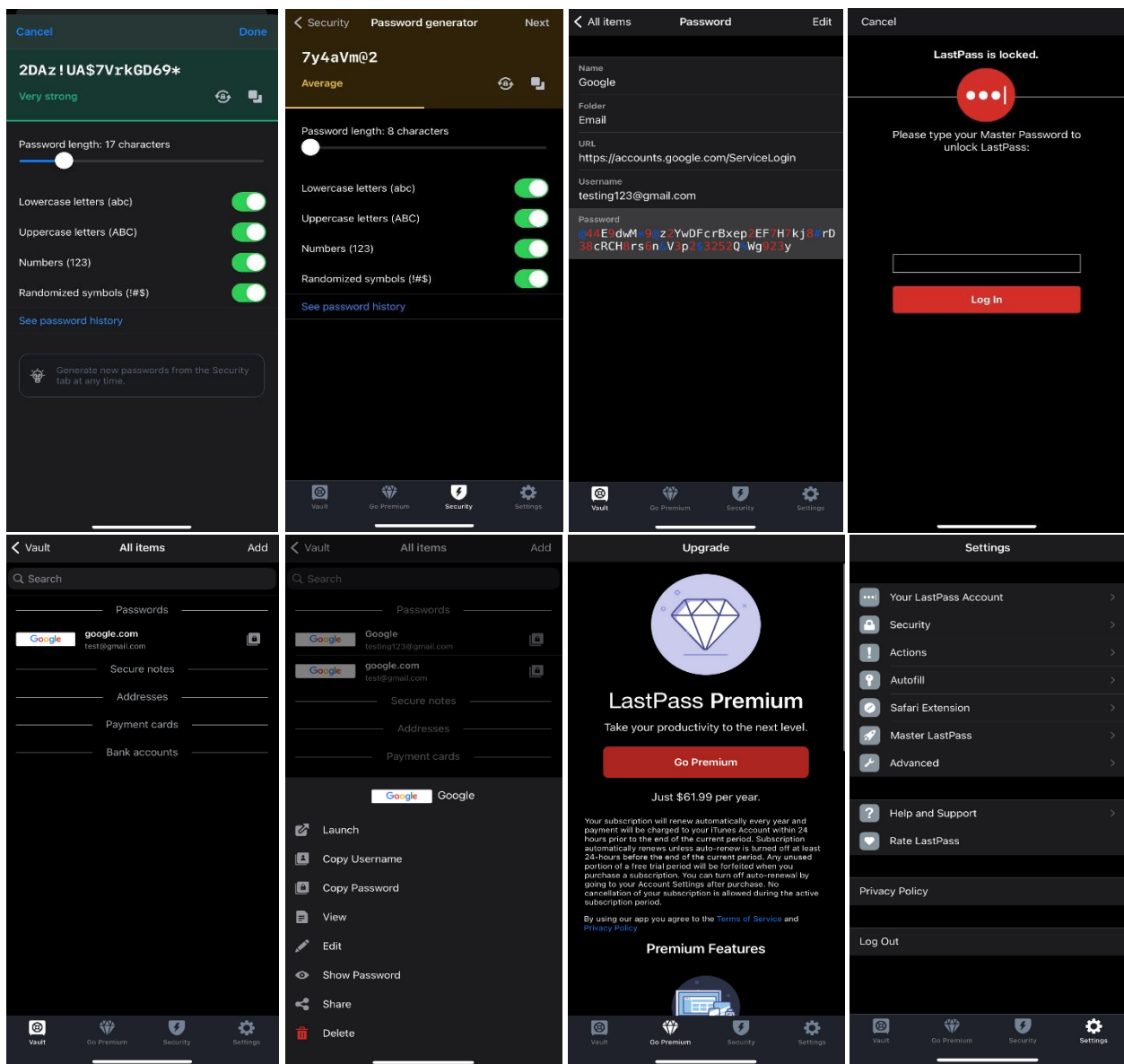
Competitor 2 – RoboForm

Competitor 3 – Microsoft Authenticator

### LastPass

**\*\*Disclaimer – All passwords and usernames used and shown are fake and are NOT real.**

Photos of images – Mobile App (iPhone)

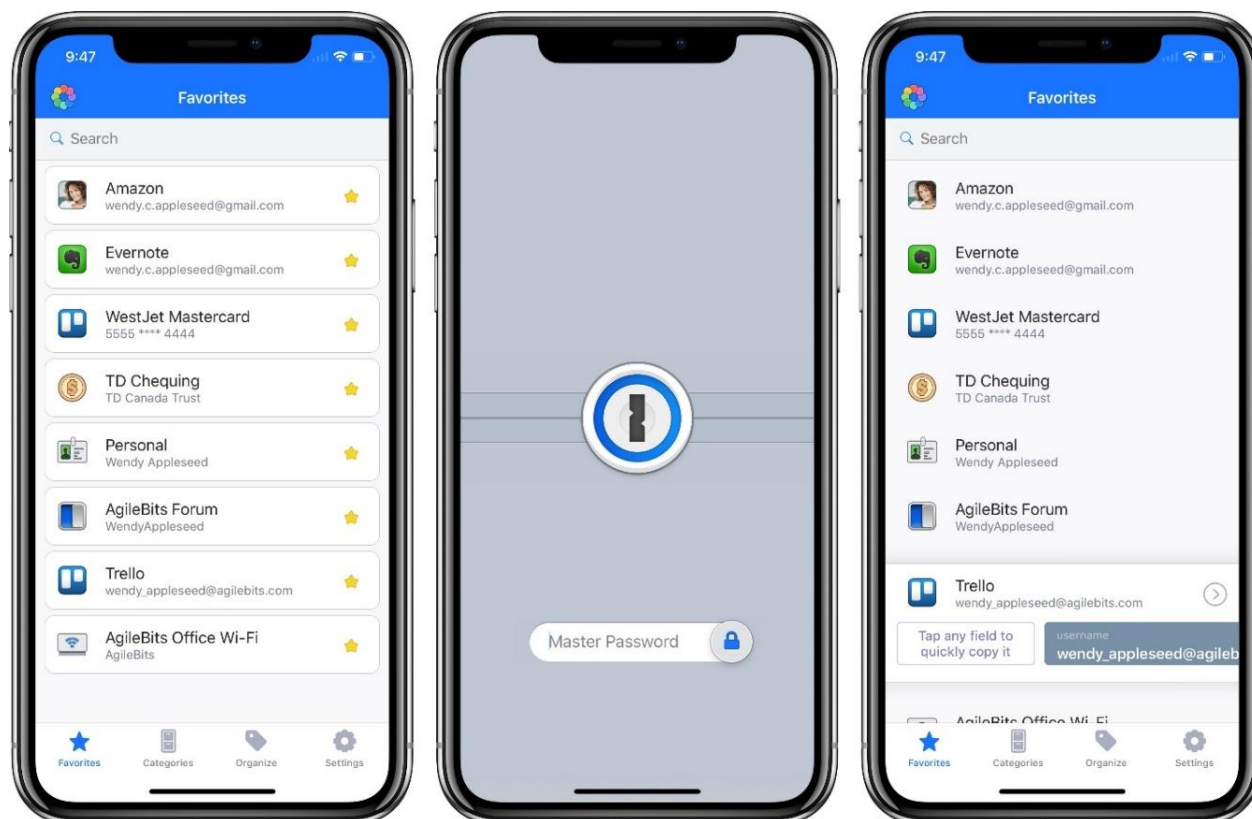


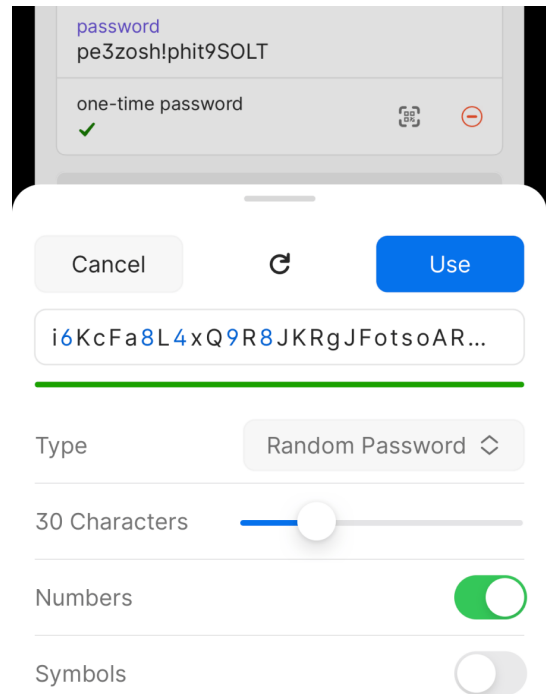
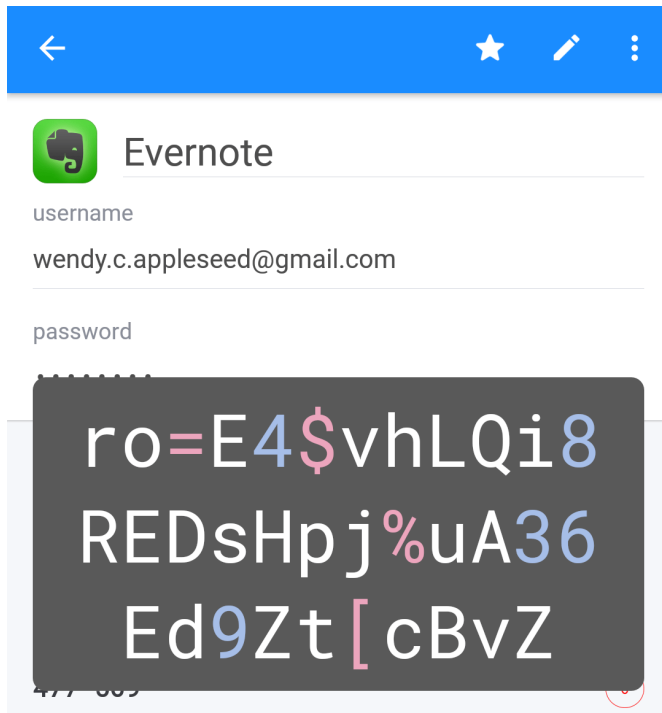
Strengths:	Weakness:	Opportunities:	Threats:
<p>Login Screen is simple and straight forward to use.</p> <p>Password Generation has a good look and feel to it.</p>	<p>Color Scheme – red and black does not look good in this application and give a warning / danger feeling subconsciously.</p> <p>Viewing Password takes at least three or more clicks which can be a pain as people would want to access it faster.</p>	<p>Color Scheme – We could redesign the color scheme by looking at color theory and making a new palette of colors for the application.</p>	<p>Go Premium</p>

One problem I faced when testing LastPass was some actions were hard to reach and hard to find. The contrast was bad as it was all similar dark colors with minimal 'standing out' buttons to press. When creating a password, you must reach all the way to the top right of the screen to press the '+' icon which made me readjust to press it. When you clicked on a login the bottom halves of the screen showed many options, but it was one of the middle options that said 'view' that I would typically want to access first without having to look for it.

Another problem I found when using the app was it was hard to read the password at times. It was too small to see long passwords, which I found to be quite frustrating and having to move the phone towards my eyes to see.

## 1Password



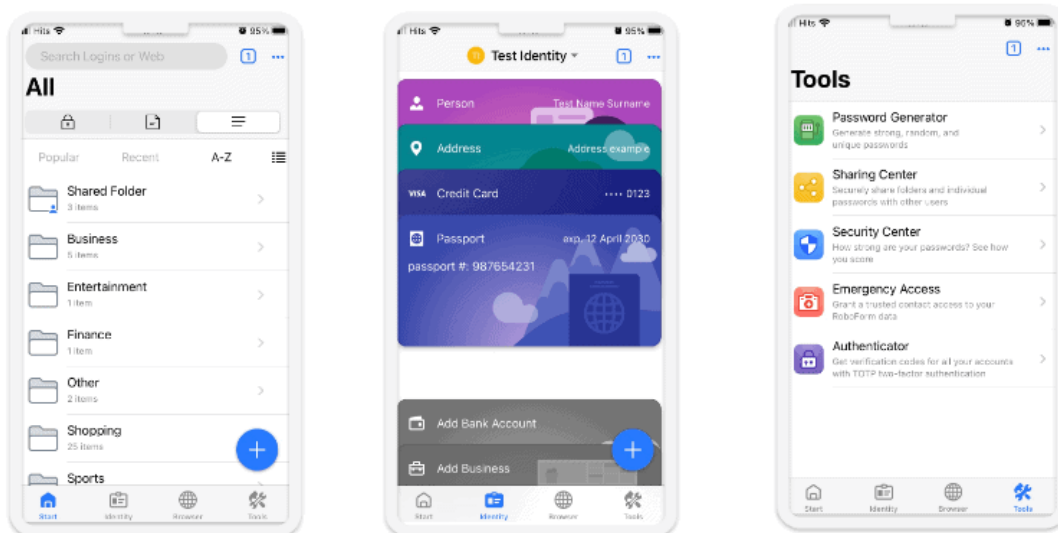


Strengths:	Weakness:	Opportunities:	Threats:
Simple easy to use interface. Multiple device compatibility. Good customer service. Ability to differentiate between distinct types of sensitive data.	Intrusive popups when performing certain tasks. Input data saving to random entries. Manually have to copy/paste info.	Allow users to autofill. Fix minor issues with functionality. Sleeker design update.	Competitors copying improvements.

One problem I faced was the amount of swiping to navigate each menu to use. Too much was going on in the creation screen and to edit the strength of the password I was generating I had to scroll each time to edit.

Another problem I faced was the pop ups when I tried to perform a task multiple time. Every so often a pop up would have to be closed to continue my task.

## RoboForm



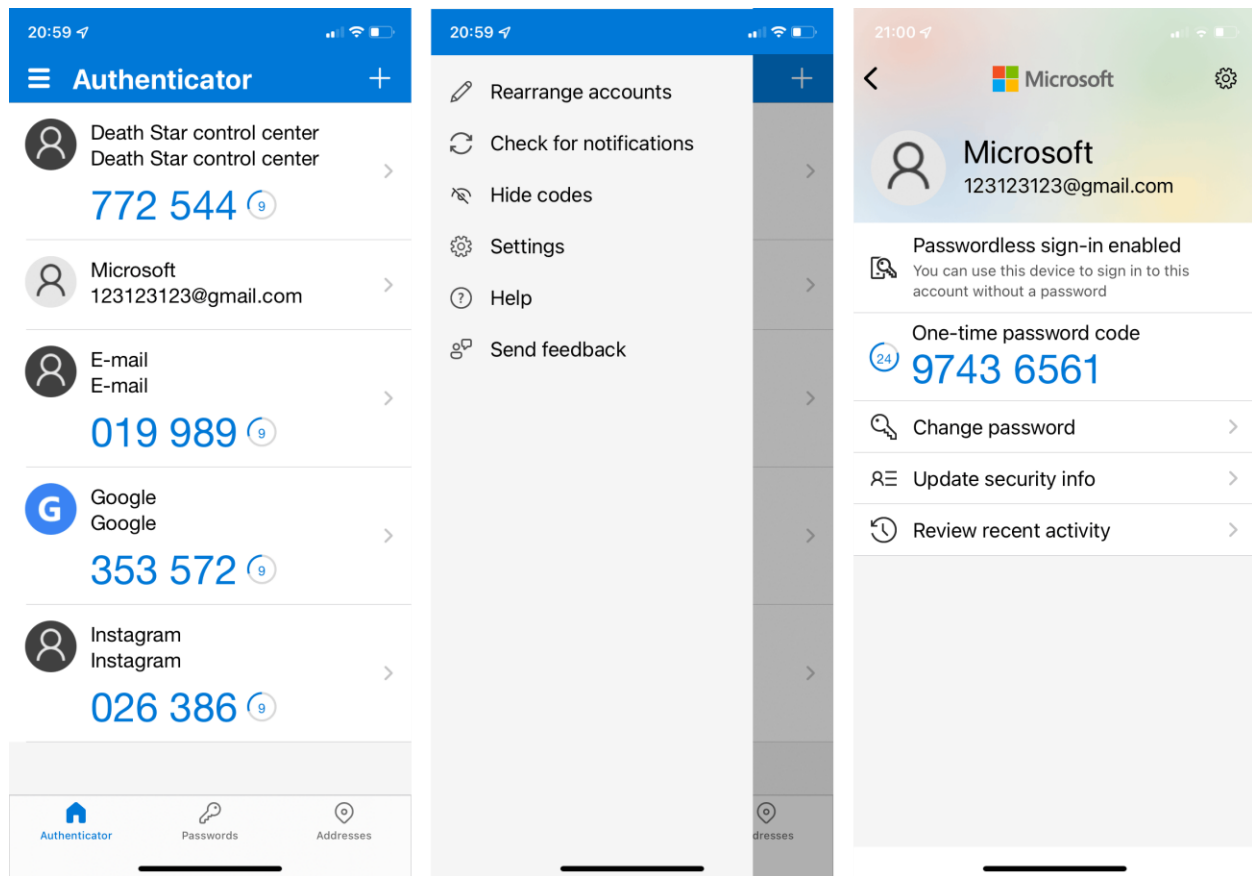
Strengths:	Weakness:	Opportunities:	Threats:
<p>Easy to use.</p> <p>Secures sensitive information well.</p> <p>Good user experience.</p> <p>Ability to randomly generate usernames and passwords.</p> <p>Multiple device compatibility.</p>	<p>Mobile use is difficult compared to desktop.</p> <p>Requires too many clicks/taps to do basic tasks.</p> <p>Autofill does not work that well.</p>	<p>Autofill to always works.</p> <p>Although there is multiple device compatibility, it would be good to be functional across all devices.</p>	<p>Security breach of sensitive data.</p> <p>Users prefer other related products.</p> <p>Too many UI updates and not enough updates for useability.</p> <p>Make you pay once you expire the free trial – unable to access any passwords until you pay.</p>

The folder experience was mediocre but mainly because I did not have a sizable number of passwords. The problem came when trying to view a password, took too long to navigate to a password when I wanted to get to it quickly.

Another problem I faced was when I clicked on a login it tried to take me to the built-in internet browser to login directly with the username and password filled out in the built-in browser. My goal was to copy the username but instead it forced me to login to the account in the built-in browser. There is a second button you can push to view the other options to copy the username, but I found this particularly frustrating considering I did not know it was going to do this.



## Microsoft Authenticator



Strengths:	Weakness:	Opportunities:	Threats:
<p>Provides an extra layer of security for users.</p> <p>Simple prompts for users.</p>	<p>Users losing main device and not being able to access other accounts.</p>	<p>Integration with other services other than Microsoft based ones.</p>	<p>Other competitors in the same field.</p>

Now this app is not designed to be a password manager, but we still investigated it for some guidance on Mobile UX. One of the problems was the list of accounts was too long as they all showed the large password. This meant lots of scrolling with lots of accounts. There is an option to change this but by default it shows all the codes.

# UI elements

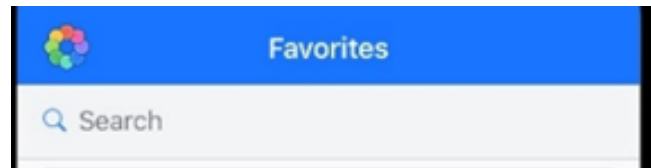
## Search-Bars

Typically, the search bar is at the top part of the screen because it is one of the first areas of the screen users will see at the top. Having a search bar allows users to easily search and find what they are looking for. This is particularly helpful for users that may have many logins and passwords saved. This is good because if users can't find their password in an accessible part of the screen then users will reach for the search bar to look for their password.

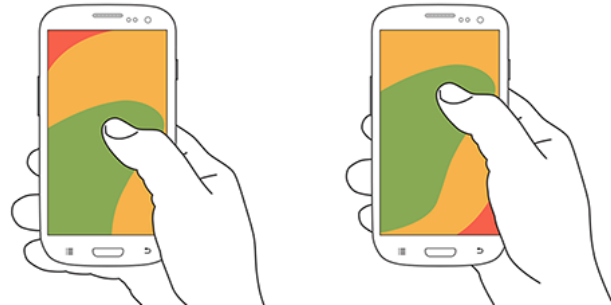
### RoboForm



### 1Password



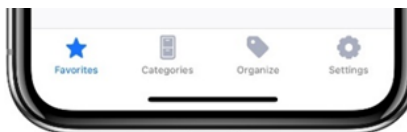
By looking at an image which shows the accessibility for using a screen with one hand we can see that the search bar is a harder to reach button because it is at the top of the screen. Although the search bars are not used a lot, this isn't a problem for the user unless they are searching for multiple passwords.



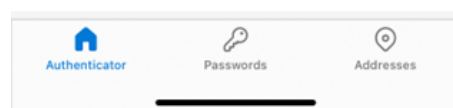
## Bottom Navigation-Bar:

Mobile apps typically have their main navigation buttons at the bottom of the app. This makes it easy for users to locate and use them because a lot of other apps use this technique. By having it at the bottom it allows more space in the top half of the UI for other information to be displayed and less cluttered. Going left to right is typically most important to least important and this is due to reachability. The thumb can reach elements on the bottom left easier than reaching for the bottom right.

### 1Password



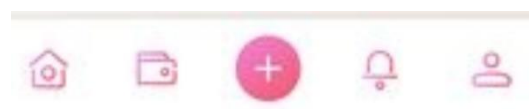
### Microsoft Authenticator



### RoboForm



### Dribbble



One thing we liked was the big '+' button in the bottom center of the screen. This would be an easy-to-get a user to create a new password and is something we will consider for the future UI/UX.



## Color Theory

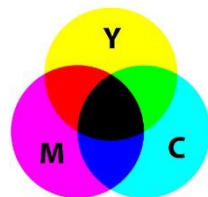
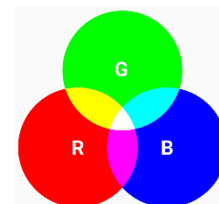
One of the problems of LastPass we found was the color scheme of the application. The contrast and colors were hard to see and did not fit the theme of a password manager, so we decided to do research into color theory to help us find a good color scheme to improve upon the UX of LastPass.

“Research reveals people make a subconscious judgment about a person, environment, or product within 90 seconds of initial viewing and that between 62% and 90% of that assessment is based on color alone.” - Source: CCICOLOR - Institute for Color Research

This is especially important as we found the color scheme of LastPass to be bad and then made that subconscious decision ourselves based on the color. We decided to look at the fundamentals of color theory to help us create a new color scheme for LastPass.

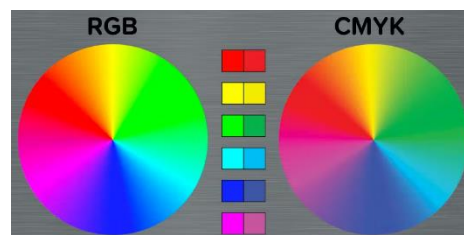
### RGB vs CMYK

RGB stands for (Red, Green, and Blue) which makes up the digital color space. Pixels on a screen can display red, green or blue pixels to make up a color range we can see with the human eye.

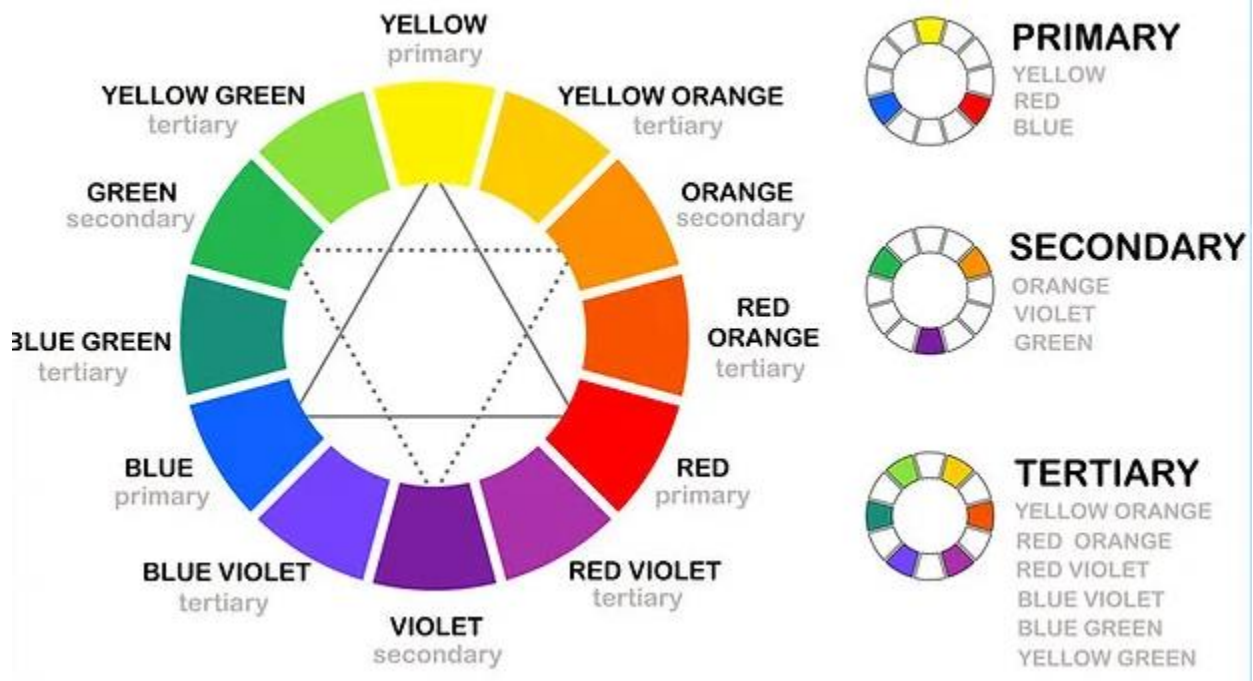


CMYK stands for (Cyan, Magenta, Yellow, Key/Black) which is used to make up physical paint colors when dealing with ink and/or printing colors.

When you use the wrong color format – changing the color format over to the application will cause the colors to change and become inaccurate as to what you meant the colors to be. Our application is digital so ***we will use the RGB color space*** to pick / use out colors.



## Color wheel

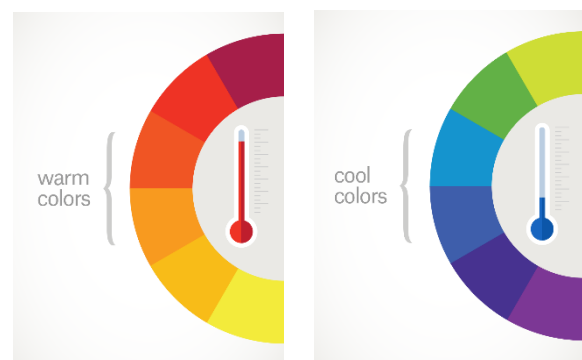


The color wheel consists of 3 types of colors. Primary, Secondary and Tertiary. The primary colors are Red, Green, and Blue from the RGB color space. The secondary colors are made by mixing the primary colors together which are Orange, Violet and Green. The tertiary colors are made by mixing Primary and Secondary colors together again which consist of the rest of the color wheel.

This color wheel is what allows us to create / select all the different colors we could want simply by mixing colors into more colors. This creates a large selection of colors but also later lets us see the color schemes work together.

There are also warm and cool colors. Warm colors are the (reds, oranges, and yellows) and Cool colors are the (blues, greens, and purples) as shown ->

Warm and Cold colors have different associations behind them such as: warm colors are associated with energy and brightness whereas cool colors are generally associated with calm and peace.



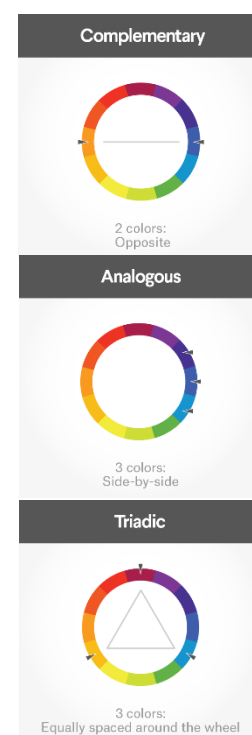
## Color Schemes

To utilize the colors effectively we follow certain color schemes that work well with each other. There are three main color schemes used to pick multiple colors together: Complementary, Analogous and Triadic. These color schemes make easy work of picking colors that work well with each other.

Complementary colors on a color wheel are opposites. This creates a sharp contrast between the two colors which can make imagery and differentiation great. However, be sure not to overuse this color scheme as it can be overused quickly if using lots of complementary colors.

Analogous colors are next to each other on the color wheel and is used to instruct people where to look. One of the colors will dominate catching the least attention as it is primarily used, one will support catching a moderate amount of attention as it is moderately used, and one will accent and catch the most amount of attention as it is rarely used. This color scheme is not nice looking but helps us direct attention to where it is needed.

Triadic colors on the color wheel are evenly spaced around. This color scheme tends to be quite energetic and powerful as it is more memorable and creates lots of contrast between the colors. Overall, this color scheme makes elements pop and stand out while maintaining the harmony of the colors used together.



## Color Psychology

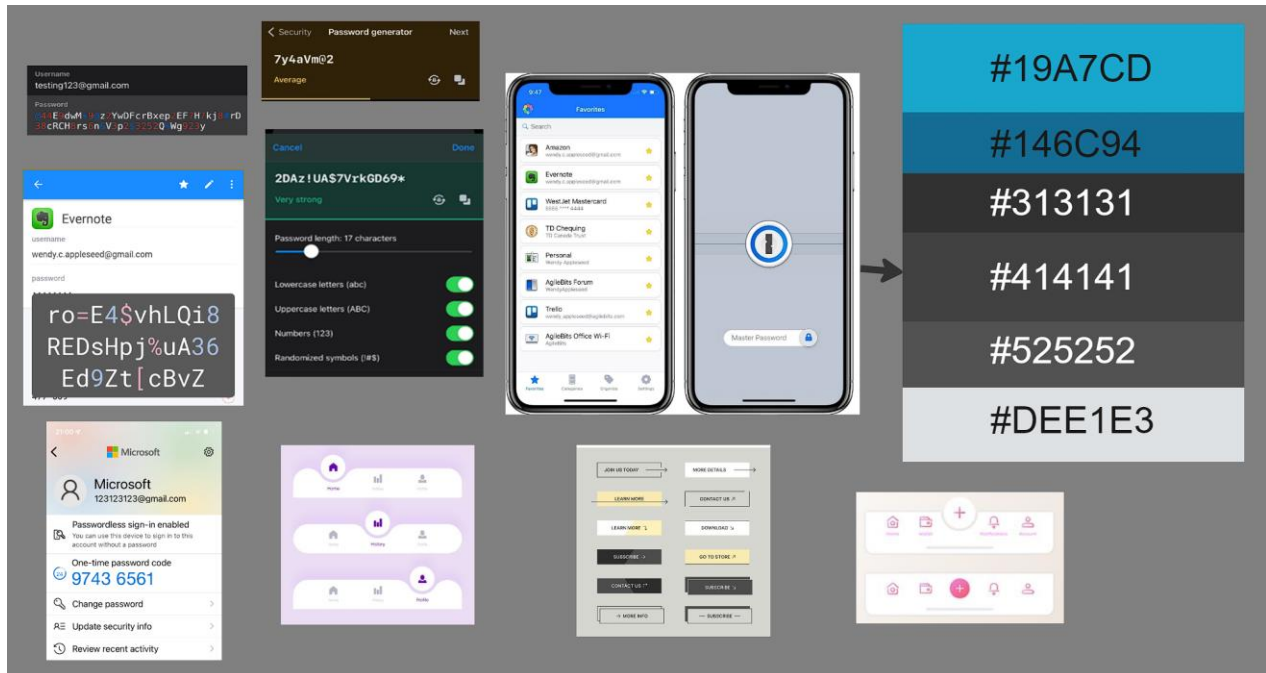
From a research article on The Application of Color Psychology – the research shows what each color represents for people. Each color will vary based on a person, but the general trend is shown below of the most common emotions / symbolic meaning with different colors.

Red	Passion – Love – Danger – Stop – Anger
Orange	Warmth – Kindness – Joy – Confidence
Yellow	Hope – Joy – Danger – Creativity – Energy
Green	Nature – Growth – Freshness – Happy – Safe
Blue	Wisdom – Hope – Reason – Peace – Trust – Loyalty – Confidence
Pink	Soft – Reserved – Compassion – Sweet
Purple	Mysterious – Noble – Royalty – Spirituality – Ambition
Brown	Dependable – Rugged – Trustworthy – Simple
Black	Cold – Noble – Formality – Dramatic – Security
White	Clean – Simplicity – Innocence – Honest – Truth – Indifference

We decided to pick a primary color based on this. LastPass is a security-based application, so we decided that BLUE as a primary color would be better as it generally gives a trustworthy and confident feeling from people. This is very different from the RED which gave feelings of danger / stop. We believe that changing the color to blue would improve the UX by making the user feel better about using the product purely based on the emotions / symbolic meaning behind the color.

# Inspiration

After looking into UI elements and performing SWOT analysis we decided to put together an inspiration board of elements we liked that we thought could help improve the UX of LastPass. We also investigated a new color scheme for LastPass after looking at color theory. We will use these to help redevelop the UX design and allow us to improve upon the design by using these design aspects as inspiration.



# User Testing Research

## Ethics

Before we start observing real people user-testing our target app (LastPass) we must consider the ethics of the testing. This is because of the amount of sensitive data we are going to be recording down, we must consider the testers' safety and consent.

We will be recording very specific information about the tester which will include:

Hand gestures the tester uses, where you touch/navigate the screen throughout each stage, eye tracking (with further consent), time taken to complete a task, pain points / difficult parts of a task and any other specific problems the tester encounters.

We will also make testers input usernames and passwords into the mobile app and because of this we need to make sure that users haven't entered their own personal usernames and passwords into the testing environment to ensure their safety.

To keep the testers safe, we created a tester consent form which all testers would require to read then sign before being tested. If the tester doesn't consent, then no test will take place. If testers revoke consent part way through, they will need to inform us, and their data will be deleted. If testers give further consent to record their eye movements – their face will be blurred / blanked out of the recording, only the eye movement is recorded.

**Research Informed Consent**

UX 105

LastPass UX Research

**PURPOSE OF STUDY**

To conduct UX Research into the mobile application LastPass, a password manager which helps users manage their passwords securely. Our goal is to redesign the app with our focus primarily on Mobile User Experience. This study will allow us to validate assumptions and create an informed plan for redesigning the Mobile App LastPass.

**RISKS**

\*\* Recorded information will include: Hand gestures the tester uses, where you touch/navigate the screen throughout each stage, eye tracking (with further consent), time taken to complete a task, pain points / difficult parts of a task and any other specific problems the tester encounters.

**\*\* This app will use sensitive data including usernames and passwords. DO NOT USE YOUR OWN INFORMATION – We will provide you with an approved list of usernames and passwords to use in this study to protect you from entering your own information accidentally.**

**CONFIDENTIALITY**

Please do not write any identifying information.

Every effort will be made by the researcher to preserve your confidentiality including the following:

- Assigning code names/numbers for participants that will be used on all research notes and documents.
- Keeping notes, interview transcriptions, and any other identifying participant information in a locked file cabinet in the personal possession of the researcher.

Participant data will be kept confidential except in cases where the researcher is legally obligated to report specific incidents. These incidents include, but may not be limited to, incidents of abuse and suicide risk.

**CONTACT INFORMATION**

If you have questions at any time about this study, or you experience adverse effects as the result of participating in this study, you may contact the researcher whose contact information is provided on the first page. If you have questions regarding your rights as a research participant, or if problems arise which you do not feel you can discuss at the time, directly contact us at the following email address [270168960@voobeestudent.ac.nz](mailto:270168960@voobeestudent.ac.nz).

**EYE TRACKING**

☐ If you consent to eye tracking tick this box.

\*\*only eye movement is recorded, the rest of the face will be blanked.

Participant's Initials: \_\_\_\_\_

Page 1 of 2

### VOLUNTARY PARTICIPATION

Your participation in this study is voluntary. It is up to you to decide whether to take part in this study. If you decide to take part in this study, you will be asked to sign this consent form. After you sign the consent form, you are still free to withdraw at any time and without giving a reason. Withdrawing from this study will not affect the relationship you have, if any, with the researcher. If you withdraw from the study before data collection is completed, your data will be returned to you or destroyed.

*Note: Please delineate the "Consent" section of the Informed Consent Form by drawing a line across the page (like this - **Example**). This delineation is important because the consent form grammar shifts from second person to first person, as shown in the example.*

### CONSENT

I have read, and I understand the provided information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I understand that I will be given a copy of this consent form. I voluntarily agree to take part in this study.

Participant's Signature \_\_\_\_\_ Date \_\_\_\_\_

Researcher's Signature \_\_\_\_\_ Date \_\_\_\_\_

Participant's Initials: \_\_\_\_\_

Page 2 of 2

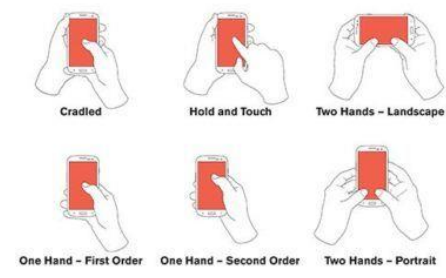
## Tasks

1. Create a username and password.
2. Find a password for account (username given to tester)
3. Go to the home area.
4. Search for the account the user made in Task 1
5. Delete username and password created in Task 1
6. Change the vaults auto lock to 5 minutes.
7. Generate a 14-character password that includes random symbols.
8. Copy and paste a saved password.
9. Lock the vault.

## Observations Recorded

- Time taken for the user to complete task.
- How the tester holds the device
- Eye Movement (If consented)
- Pain points / confused moments the tester experiences.

When measuring how a tester holds a device, we will refer to the diagram below to ensure constant definitions. Results can be either one or a combination of the following holds that a user is able to hold a phone while using the app to complete a task.



## Interview Questions

### Open Questions

1. What features or functions of the app that you found confusing or difficult to use?
2. What features or functions of the app that you found particularly helpful?
3. How important is password strength and security to you when using an app like LastPass?
4. What do you think about the color scheme of the app?
5. What buttons stood out the most to you while using the app?
6. How did you feel about the overall design and layout of the app?
7. What would you change about the app?
8. Is there anything else you would like to add about your experience with the LastPass mobile app?

### Closed Questions

1. On a scale of 1-10 how hard was all the tasks?
2. Did the app feel secure to you?
3. Did it feel easy to navigate the app?
4. Was finding a password you looked for fast enough for you?
5. Did you like to color scheme of the app?

## Results

The raw data results are as follows:

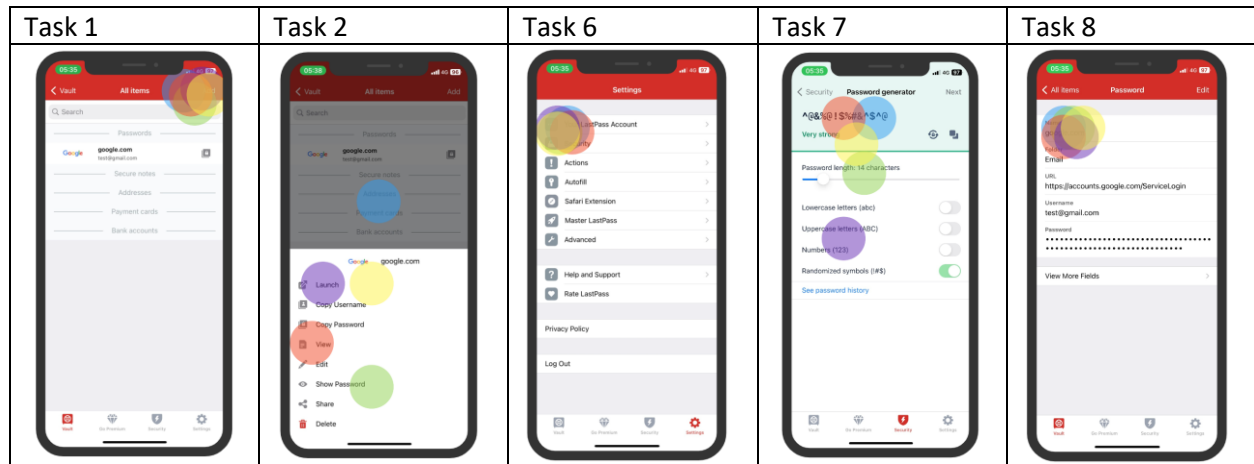
Time Taken	User 1	User 2	User 3	User 4	User 5	Average
Task 1	23s	26s	25s	39s	26s	27.8s
Task 2	5s	15s	7s	19s	13s	11.8s
Task 3	11 sec	13 secs	12 secs	12 secs	13s	12.2s
Task 4	5s	8s	7s	6s	5s	6.2s
Task 5	Error*	Error*	Error*	Error*	Error*	N/A
Task 6	10s	16s	17s	16s	20s	15.8s
Task 7	14s	21s	24s	23s	24s	21.2s
Task 8	10s	14s	13s	14s	11s	12.4s
Task 9	1s	10s	5s	15s	10s	8.2s

\*Upon getting the users testers to perform task 5, the application failed to complete the task due to technical error of the application. This was not user error and the behavior of the delete button did not complete the proper functionality.

Device Hold	User 1	User 2	User 3	User 4	User 5
Task 1	One hand-first and second order and cradled	One hand-first and second order and cradled	One hand-first and cradled	One hand-first and second order and cradled	One hand-first and second order and cradled
Task 2	One hand-first order	One hand-first order	Cradled	One hand-first order	One hand-first order
Task 3	One hand-first order	One hand-first order	Cradled	One hand-first order	One hand-first order
Task 4	One hand-first + second order	Cradled	Hold and touch	One hand-first + second order and two hands portrait	One hand-first + second order and two hands portrait
Task 5	One hand-first and second order	One hand-first	Hold and touch	One hand second order	One hand-first and second order
Task 6	One hand-first	One hand-first	Hold and touch	One hand-first	One hand-first
Task 7	One hand second order	One hand second order	Hold and touch	One hand second order	One hand second order
Task 8	One hand-first and second order	One hand-first and second order	Cradled	One hand-first and second order	One hand-first and second order
Task 9	One hand-first order	One hand-first order	Hold and touch	One hand-first order	One hand-first

Where the tester first looked when asked to perform a task:

\*\* Not all tasks were measurable. Each tester is represented by the colored circle.



Pain points / confused moments the testers experienced:

- When looking for the password with the login opened (not the pop up) the users all look from the top down to find their passwords. The unnecessary data at the top / beginning where all the users looked first slowed the user down as they scanned the lines like a book to find their password.
- When looking for the password with the login pop up (not the subpage) the users all look from the top down to find their passwords. The unnecessary buttons at the top / beginning where all the users looked first slowed the user down as they scanned the lines like a book to find the correct button to view their password.
- When deleting a login, it would remain in the application (unexpected behavior) and the testers all stopped confused what to do. We then stopped the tester after their attempt to delete the login.
- Some tasks required users to change hand grips multiple times because of the placement of some buttons. However, we noted down that none of the testers complained or struggled with this as they were familiar with doing it. For example, when searching for a login the keyboard popped up and the users were all familiar with changing hand positions to type on the keyboard.



## Open Questions

What features or functions of the app that you found confusing or difficult to use?

- *"Delete a password didn't work, even after trying a few times which was unhelpful because the button said "delete" and it just loaded and did nothing."*
- *"When you touch a login, it brings up a pop-up menu, but is frustrating to use as the order is not helpful and you have to search through it to look for the more 'helpful' options."*
- *"The view password button brings the password up, but it is too small to read easily."*
- *"When in a login page to view all the details, the first two pieces of information you look at are irrelevant and not the username and password you expect which causes longer search times"*
- *"When you create a new login, it auto populates the LastPass logins email address which is frustrating because I have to delete it every time to create a login."*

What features or functions of the app that you found particularly helpful?

- *"The contrast between the pop up and the background was good and help direct my eyes to the different options available."*
- *"The add and search functions were exactly where I expected them to be! Also, when creating a password, the color in the password generator works well and is easy to follow."*
- *"I would expect add/edit/done buttons to be in the top right and they were (:"*
- *"Searching for a password is easy with the search bar"*
- *"The app has familiar navigation points like bottom nav bar with easy to reach buttons and makes great use of the screen to space the elements of the app out nicely"*

How important is password strength and security to you when using an app like LastPass?

- *"I think that it is important that the app is secure and won't leak my passwords. Plus, I don't want to be hacked by using a weak password."*
- *"If the app didn't look secure then I probably wouldn't use it. LastPass is something I would use based on what I have tried. My passwords probably aren't the best but they are secure enough for me so that doesn't matter too much if they aren't leaked, I guess."*
- *"Well, it is storing MY private information so extremely important! My private info needs to be secure or just not be there in the first place so yes password strength is also quite important for more sensitive applications in my opinion when involving money and personal information."*
- *"I think that having a string password isn't a must but shouldn't be something too simple like 'password'. For the app I would assume the app I am using would already be secure and doesn't really worry me."*
- *"Meh it is what it is. It is not too hard to reset an account's password in today's world with email reset. I would hope that what I am using is secure but yes doesn't bother me."*

What do you think about the color scheme of the app?

- *"Eh the red, black and white isn't my thing. The different colors when reading a password is pretty good though, make it much simpler to read."*
- *"I personally use one password and prefer blue over red but that's just a personal preference. Blue is one of my favorite colors to be fair."*

- *"The red gives off some weird vibe to it, but I don't mind it either way. It is, however, VERY simple, almost too simple of a color scheme. Feels like something is missing you know?"*
- *"It's bland and red isn't the best base color in my opinion, but it looks fine with what they have done with it."*
- *"Well, I am not fused like it is simple enough to use but nothing really stands out as good except for generating a password. The colors used there are good feedback when making a password."*

What buttons stood out the most to you while using the app?

- *"Mainly the bottom navigation buttons, as they were always there wherever I was in the app"*
- *"When going to create a new login I looked where I would typically go to create something and that was the top right. Although it didn't stand out, it was muscle memory, and I tapped the 'new' button without even reading which did exactly what I was expecting."*
- *"In the security tab there is a button for generating a password. This one stands out as it is the first option and a very clear button with a symbol and writing."*
- *"When looking for the delete button, it was quick and easy to find because it was a different color than the rest (red) and stood out from all the standard buttons."*
- *"The settings button was easy to find as it was in a place, I would expect in the bottom nav bar."*

How did you feel about the overall design and layout of the app?

- *"The design is useable, but some things take longer than they should like viewing a password because of extra steps needed to access it."*
- *"The order of some items was annoying to navigate but overall, the design was okay... If they ordered the buttons from importance and took out the unnecessary content, it would be better."*
- *"It's okay, it feels a little bit messy to use but is overall it achieves most of its needs and goals."*
- *"The app needs some tweaking to make it better, there are some features that I think are missing, but that's okay overall its useable but I feel like the app is not designed around everyday users and more larger consumers like businesses."*
- *"It does its job and stores logins, but the useability feels a bit shoddy to me. If they changed little things, I'm sure it would come a long way."*
- *"I mean it feels okay to use but could definitely use some improvements to make it feel easier to use in my opinion."*

What would you change about the app?

- *"I would like to see a faster way to access already saved passwords because if I were to use this in reality, I wouldn't want to click multiple different times and areas to access the password."*
- *"A way to lock the app with a button would be nice. The only way to lock it that I could find was to leave the app itself."*
- *"An option to view a larger password like they have in 1Password would be good. I use 1Password for my passwords and the feature is useful."*
- *"I am not sure, there is nothing specific that comes to mind."*
- *"A button to paste in the main users email instead of it being prepopulated and having to delete it EVERY time you make a new login would be nice."*

## Closed Questions

Questions	User 1	User 2	User 3	User 4	User 5
On a scale of 1-10 how hard was all the tasks?	7	6	6	8	7
Did the app feel secure to you?	Yes	Yes	Yes	Yes	Yes
Did it feel easy to navigate the app?	Kind of	Yes	Kind of	Yes	Yes
Was finding a password you looked for fast?	No	Yes	Yes	Yes	Yes
Did you like the color scheme of the app?	No	No	No	Don't Care	No

## Limitations of testers

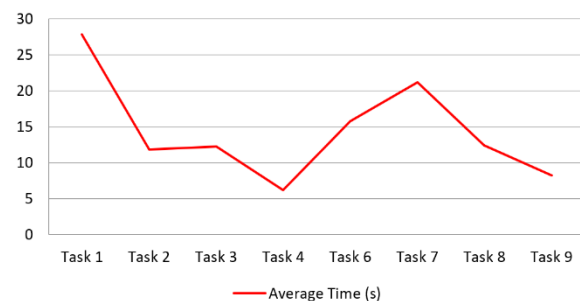
We do acknowledge that we only had 5 testers in our testing. This was due to time constraints we couldn't get any more done within the required time, however we believed with a minimum of five testers we would be able to make accurate inference based on our results. We also acknowledge that our testers were only those that fell within our target audience. We realize that it does skew our results, however we are targeting this research based on our target audience, so all the data remains accurate for what we tested for.

# Data Analysis

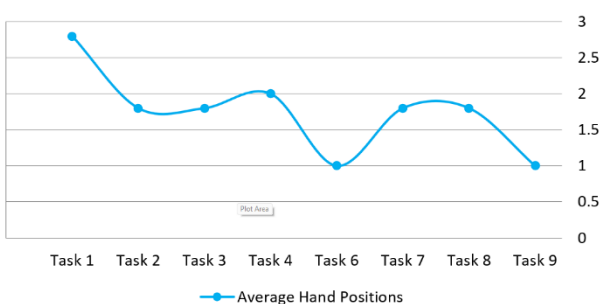
## Graphs

Between the 5 testers, we decided to plot the average time for each task for all the testers. This indicates to us that tasks are more time-consuming than others. Particularly task 1 and task 7 which were creating a login and generating a 14-character password of symbols respectively. These two tasks represent some of the core features that users will be using in the real world as it what the app is designed to do. This allows us to see where we should focus on improving the UX by making sure that key features aren't hard to use and are generally fast for users to complete.

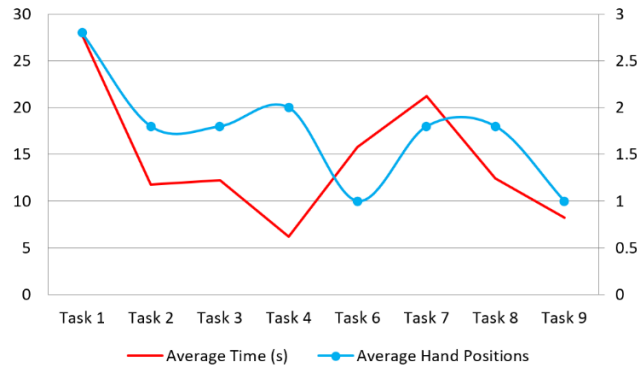
**Average Time (s)**



**Average Hand Positions**

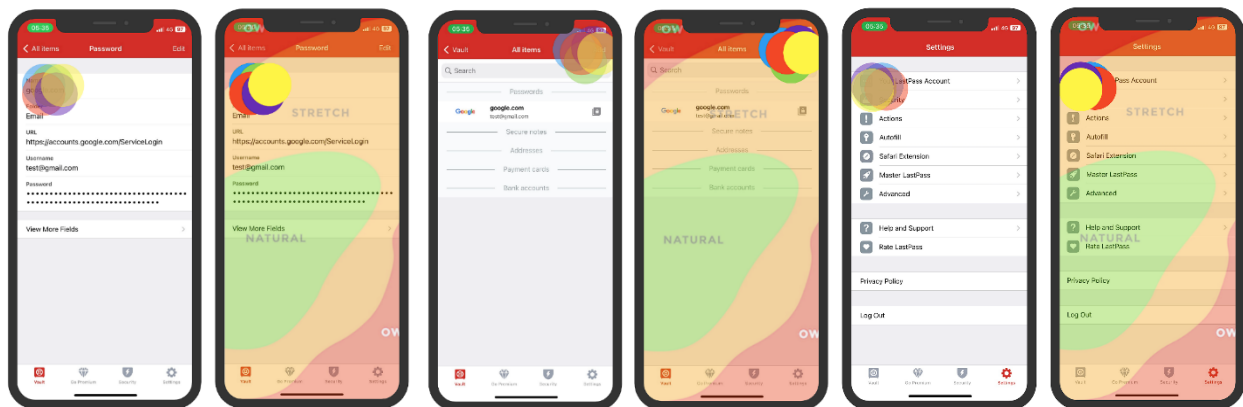
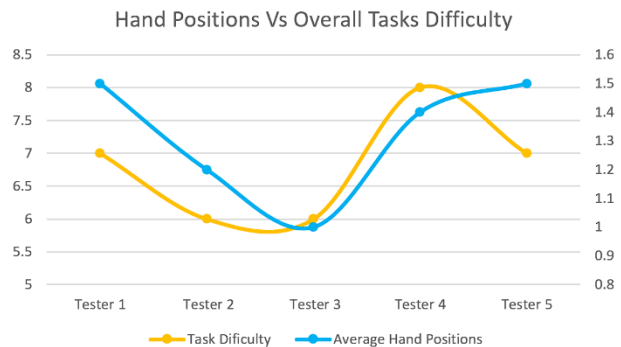


Next, we plotted the average hand positions the testers used for a given task. We can see a similar trend to the average time per task with task 1 having the most different hand positions used on average to complete a task. In this case creating a login. This indicates again that there is something wrong with the UX of the creating a password because of the amount of hand positions on average needed to complete the task.



We decided to combine the graphs when we saw how similar they were. This graph now indicates to us that there tends to be a relationship between the time it takes to complete a task on average and the amount of hand positions that were needed to complete a task. This will also allow us to see how to improve tasks by showing that we could try reducing the number of different hand positions needed to reduce time per task.

Another graph we decided to make was one that showed the individuals testers average hand positions used for every task and how difficult the user felt the tasks were overall. This indicates to us that some testers found the tasks more difficult when they used more hand positions on average. However, we understand that not everyone is going to use the app the same and have the same experience. So, we will use this data as an indication to reinforce our other data sets.



All our testers consented to eye tracking where we recorded the first place a user looked at when opening a new page to complete a task. These are three results shown first as the normal app with all the users first looks and then a second one with an overlay showing the thumb reachability. We first noticed that the users all looked in the same spot because they were expecting the option to be where they looked. Although this is true for some of the cases, the first image shows the tester looking for a username + password but found some unneeded data instead. We also experienced this issue when performing SWOT analysis on the app. The data also indicates to us users won't look somewhere they can't reach typically when they are first looking for the button or option they need.



The data also shows us some outliers when it came to the first place a tester looked. When clicking on a password to view it, a menu comes up and the testers didn't expect this or know where to look. We can still see that users typically look within areas they can reach but this time users didn't all look in the place. However, most users looked in the same general area still which is an indication to us how a user might search for something on a screen. The other screen was the password generator. This was a new screen for the testers as they had never seen it and were told to generate a 14-character password of symbols. We can see that the first looks are closer together and still within the reachability of the thumb for a user.

## Card Sorting

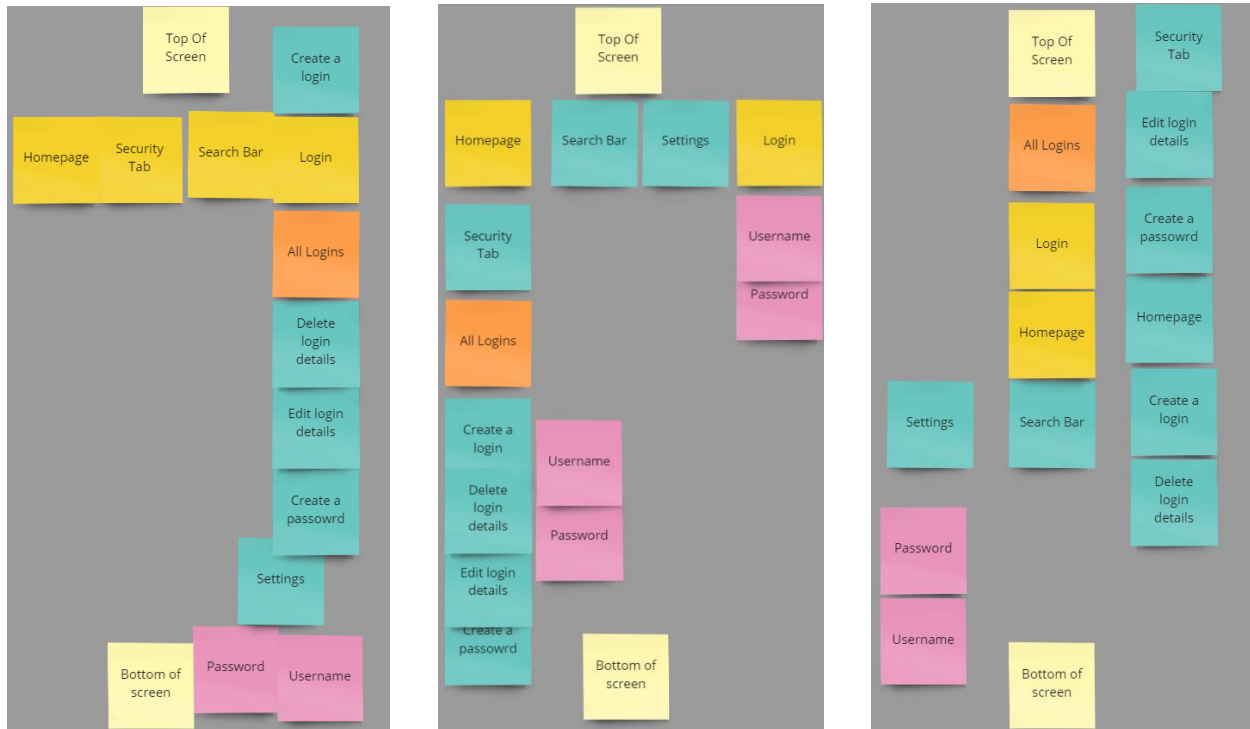
We decided on the key parts of the LastPass that were the key / fundamental parts that made it a whole which were:

- Navigation with (Top and Bottom of the screen).
- Search bar.
- Creating a login.
- Home page.
- View login page.
- Settings.
- Security tab.
- Create a password.
- All logins.
- Delete login details.
- Edit login details.
- Password.
- Username.

We then arranged the cards based on what they did and the closer together cards were, the more they linked to each other in any way. Our results are indicated here ->

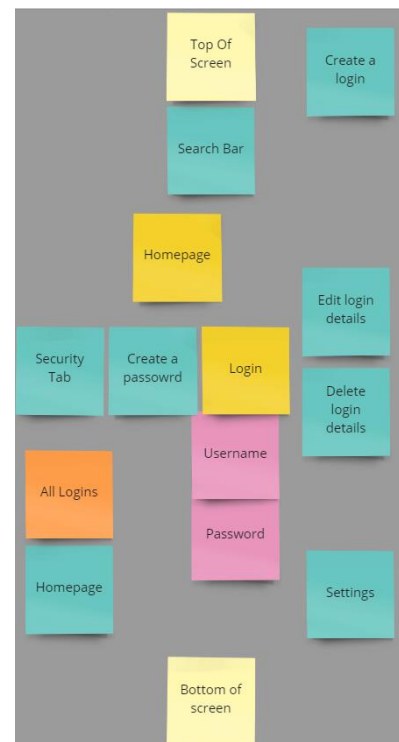


By having done the card sorting we can use this to visualize the key aspects and how they link together to make LastPass a whole. However, we realized that this may not be how everyone would have organized the cards like we had. So, we decided to get 4 other groups of software developers doing similar research to us to do card sorting with the same cards and see the results to make it fairer and more accurate.



Although the results are NOT the same for every card sort, we were expecting this because not everyone is going to categorize and sort the information in the same way. However, we can from all 5 of the cards sorting results categorize common areas that were apparent in all results.

- Username, password, and some type of login details or actions were put together.
- Create a login was placed near the top of the screen.
- All logins were paired with create, edit, delete login details.
- Home page typically paired with all logins.
- Search bar was placed at the top of the screen generally.



# Assumptions Revisited

## Security and Privacy:

***We assume that users think that the platform is secure and reliable to store and access their data. We assume users believe their data is safe within this app as it will have security features, including advanced encryption and/or multi-factor authentication, to ensure that users' data is protected from unauthorized access. As the app being researched is designed to store sensitive information, it is crucial we focus on security and privacy.***

- All our testers commented on app security when using a password manager like LastPass. Generally, the results were users believed that the app would be secure as it dealt with their private information and unanimously told us that security and passwords were important, especially if it contained their personal information. From this we conclude that our assumption here is valid and accurate.

***We assume that users don't want their passwords being shared - as this would allow other people to login to that user's account. From this assumption we know that the app we are making will need to be secure so that only the user can access its data and not others.***

- The comments from our 5 testers went between being important and not caring. Some didn't really seem too worried about it but made the comment "I would hope that what I am using is secure but yeah doesn't bother me." Whereas other testers thought it was very important their passwords weren't shared because it could reveal their personal information. Therefore, we are generally going to say that this assumption is true and sort of false as most users care but some don't.

## Ease of Use:

***We assume users want to access their passwords as fast as possible while maintaining the security factor. We assume users know how to copy and paste their passwords on their mobile device. We want to make the UI/UX as easy/straight forward as possible to help users access their passwords when needed.***

- Our results showed us a trend that allows us to see that tasks took longer than others. There was a trend that shows longer tasks typically required the user to switch hand positions more often than short tasks. When asked if the testers found the tasks hard on a scale of 1-10, the results showed us that the testers who found the tasks more difficult used more hand positions than others. All the users managed to copy and paste a password without help so we say that our assumption here is correct that users know how to copy and paste on their device and want an easy/straightforward process to do so.

***We assume users will need to import or create a username/password for every one of their existing accounts when first using the app, because of this we believe that it is important to make the creation/editing of usernames/passwords as simple and straightforward as possible to make it a less tedious task than it must be.***

- No data was gathered to correctly identify if this assumption is true or not, however we know that from our target audience research, everyone who answered the survey has used a password manager before, whether it was saving a password in their phone / browser or a specific app for it. We believe that if you are transitioning to a new password manager, you are going to need to

import all your logins from personal experience moving passwords from one password manager to another.

## **Compatibility:**

***We assume users will be working on various platforms and different types of mobile devices from Android phone, Apple iPhone, Windows phone and/or Google phone. From this assumption we need to make sure that we account for as many different devices as we can and make it compatible with them, so the mobile app works the same on every device as expected.***

- We didn't collect data on what type of device our testers used or what devices our target audience used because there are too many mobile devices out there. We know that the majority of mobile devices have different screen sizes and constraints which is why we added this assumption. Although we can't validate it with data, we are certain from experience that we will need to make sure that the app works for any type of screen it comes across for a mobile device.

***We assume using users will be using a touch screen on their device, so we will need to take this into account when designing the UX/UI for the mobile app as there are multiple factors that can make it hard to use a touch screen including but not limited to small buttons and inconsistent UI.***

- Our target audience is the younger generation of adults and older teenagers. We don't know for certain what type of device EVERYONE will be using, but we know that if the device the user has contains the Google, Apple, or Android app store then it will be a touch screen device. All our personas have touch screen devices, and we are certain that users will have a touch screen device to use this app or won't use this app on their mobile device at all.

***We assume most mobile devices are handheld and/or fit in a pocket. This means that text size and contrast is going to be important for the user to read on the mobile device easily.***

- All our testers had mobile devices which came out of their pockets. Although this can have external factors like small pockets or large phones, typically an average mobile device will fit in the user's pocket. Although there is no data on this in this report, we are certain that the average mobile device will fit in an everyday user's pocket from our target audience.



# Conclusion

## Final App Needs

Here are the following improvements and changes for the Mobile UX of LastPass:

- Decrease the time it takes to create a login. – From our user testing and swot analysis we found that the time that it takes to create a login was much longer than other tasks performed by the testers on average. By making it shorter, we are ensuring that the users need to quickly create a password will be focused on.
- Make it when you click on a login, it brings you straight to the details page with username and password instead of a menu popup. – Testers noted that the popup menu made the menu feel cluttered and up in your face. We suggest that having it go straight to the details page instead of a popup would be a better use of UI and design principles.
- Change the color scheme into something more appealing to users. – From SWOT analysis we found the color scheme that LastPass uses did not suit the requirements. We did research into color theory and decided on a new base color blue would work better than red due to subconscious feelings when you see the color. Most of our testers also disliked the color scheme of LastPass after evaluating the mobile app.
- Remove the 'Premium' option from the main navigation menu. – We found from SWOT analysis that the Premium button felt like bloatware rather than a nav option. We believe this is not the place for the premium button and think it is better under the options menu. This will also help users quickly navigate the bottom nav bar faster as they will not need to go past this hardly used option.
- Add a lock button functionality. – From the user testing, we found that users were having a challenging time trying to find the lock button functionality. Having a lock button on the navigation bar will make it easier for the user to find.
- Add a more reachable create login button on the main navigation bar. – Looking at the User testing we saw that users were taking around an average of 28.13s to create a login, by having a create login button on the main navigation bar we can cut this time down significantly. Which will accommodate for the user's and business needs.
- Make navigating to view a password easier by decreasing the number of touches needed. – Currently you need a minimum of 3 touches to access a password. We want to reduce this number and decrease the amount of distance between each action to make it easier to navigate and access the password quickly to accommodate the user's needs.

## Final Plan

The plan from here is to redesign LastPass into a faster and easier to use password manager.

We will meet the business needs by ensuring that users privacy is the first priority when it comes to the application. We will maintain or even increase the reputation of LastPass by redesigning the mobile application into a better application than it already was. We ensure the password manager will remain secure by encrypting the users' data and using the already in place security.

We will meet the users' needs by redesigning the UI/UX to make it faster and more straightforward to use key features of the mobile app. This includes making the process to read/copy/edit/create logins faster. We will also change the color scheme of LastPass to make the app feel more secure to the user subconsciously.

We will add all the improvements into LastPass UX mentioned above to ensure that the business and users' needs are both met. Any other details that need to be changed while developing/redesigning LastPass must consider the research we conducted for the better interest of the business and user needs.

# Timeline

CS104

Workspace visible

Board

ToDo

Assumptions

Target Audience Survey Questions

Target Audience Survey Results

Target Audience Survey Research

SWOT - RoboForm

SWOT - TBC

Inspiration

+ Add a card

Doing

SWOT - 1PASSWORD

SWOT - Original (LastPass)

+ Add a card

Done

Initial document setup

Discussion with client

Business needs

User needs

+ Add a card

TimeFrame

Start of Project

Objective & Strategy

Research

Data Analysis

Conclusion

End of Project

+ Add a card

CS104

Workspace visible

Board

ToDo

UI Elements

+ Add a card

Doing

Target Audience Survey Research

Inspiration

+ Add a card

Done

Initial document setup

Discussion with client

Business needs

User needs

SWOT - 1PASSWORD

SWOT - RoboForm

SWOT - Microsoft Authenticator

SWOT - Original (LastPass)

Assumptions

Target Audience Survey Questions

+ Add a card

TimeFrame

Start of Project

Objective & Strategy

Research

Data Analysis

Conclusion

End of Project

+ Add a card

Waiting

Target Audience Survey Results

+ Add a card

**ToDo**

- UI Elements
- Further Explanation for SWOTS
- Qualitative open questions (Mobile App) - Survey
- Quantitative closed questions (Mobile App) - Survey
- APA Referencing
- + Add a card

**Doing**

- Observations
- Inspiration
- Personas x 3-Will write 3 of them
- + Add a card

**Done**

- Initial document setup
- Discussion with client
- Business needs
- User needs
- SWOT - 1PASSWORD
- SWOT - RoboForm
- SWOT - Microsoft Authenticator
- SWOT - Original (LastPass)
- + Add a card

**Done (Continued...)**

- Assumptions
- Target Audience Survey Questions
- Target Audience Survey Research
- Ethics
- Target Audience Survey Results
- + Add a card

**TimeFrame**

- Start of Project (Mar 2)
- Objective & Strategy (Mar 12)
- Research (Mar 15)
- Data Analysis (Mar 17)
- Conclusion (Mar 20)
- End of Project (Mar 23)
- + Add a card

**ToDo**

- Presentation
- APA Referencing
- + Add a card

**Doing**

- Analysis Data
- Card Sorting
- + Add a card

**Done**

- Initial document setup
- Discussion with client
- Business needs
- User needs
- SWOT - 1PASSWORD
- SWOT - RoboForm
- SWOT - Microsoft Authenticator
- SWOT - Original (LastPass)
- + Add a card

**Done (Continued...)**

- Assumptions
- Target Audience Survey Questions
- Target Audience Survey Research
- Target Audience Survey Results
- Ethics
- Personas x 3-Will write 3 of them
- Further Explanation for SWOTS
- Inspiration
- Color Theory
- + Add a card

**Done (Continued 2.0...)**

- UI Elements
- Observations
- Qualitative open questions
- Tester Tasks
- Quantitative closed questions
- + Add a card

**TimeFrame**

- Start of Project (Mar 2)
- Objective & Strategy (Mar 12)
- Research (Mar 15)
- Data Analysis (Mar 17)
- Conclusion (Mar 20)
- End of Project (Mar 23)
- + Add a card

CS104 Workspace visible Board

**ToDo**

- Presentation
- Conclusion
- + Add a card

**Doing**

- Analysis Data (AL JS)
- Re Assumptions (JS)
- Final App Needs
- Final Plan
- + Add a card

**Done**

- Initial document setup (AL JS)
- Discussion with client (JS)
- Business needs (AL JS)
- User needs (AL JS)
- SWOT - 1PASSWORD (JS)
- SWOT - RoboForm (JS)
- SWOT - Microsoft Authenticator (JS)
- SWOT - Original (LastPass) (AL)
- Assumptions (AL JS)
- + Add a card

**Done (Continued...)**

- Target Audience Survey Questions (AL)
- Target Audience Survey Research (AL JS)
- Target Audience Survey Results (AL JS)
- Ethics (AL JS)
- Personas x 3-Will write 3 of them (AL JS)
- Further Explanation for SWOTS (AL JS)
- Inspiration (AL JS)
- Color Theory (AL)
- Card Sorting x4 more (AL)
- + Add a card

**Done (Continued 2.0...)**

- Explanation of Graphs (AL)
- UI Elements (AL JS)
- Quantitive closed questions (AL)
- Observations (AL JS)
- Qualitive open questions (AL)
- Tester Tasks (AL JS)
- Graphs (AL)
- APA Referencing (AL)
- Card Sorting Explanation (AL)
- + Add a card

**TimeFrame**

- Start of Project (Mar 2)
- Objective & Strategy (Mar 12)
- Research (Mar 15)
- Data Analysis (Mar 17)
- Conclusion (Mar 20)
- End of Project (Mar 23)
- + Add a card

CS104 Workspace visible Board

Power-Ups Automation Filter AL JS Share

**Doing**

- Presentation (AL JS)
- + Add a card

**Done**

- Initial document setup (AL)
- Discussion with client (JS)
- Business needs (AL JS)
- User needs (AL JS)
- SWOT - 1PASSWORD (JS)
- SWOT - RoboForm (JS)
- SWOT - Microsoft Authenticator (JS)
- SWOT - Original (LastPass) (AL)
- Assumptions (AL JS)
- + Add a card

**Done (Continued...)**

- Target Audience Survey Questions (AL)
- Target Audience Survey Research (AL JS)
- Target Audience Survey Results (AL JS)
- Ethics (AL)
- Personas x 3-Will write 3 of them (AL JS)
- Further Explanation for SWOTS (AL JS)
- Inspiration (AL JS)
- Color Theory (AL)
- Card Sorting x4 more (AL)
- + Add a card

**Done (Continued 2.0...)**

- Explanation of Graphs (AL)
- UI Elements (AL JS)
- Quantitive closed questions (AL)
- Observations (AL JS)
- Qualitive open questions (AL)
- Tester Tasks (AL JS)
- Graphs (AL)
- APA Referencing (AL)
- Card Sorting Explanation (AL)
- + Add a card

**Done (Continued 3.0...)**

- Analysis Data (AL JS)
- Re Assumptions (AL JS)
- Conclusion (AL JS)
- Final App Needs (AL JS)
- Final Plan (AL JS)
- + Add a card

**TimeFrame**

- Start of Project (Mar 2)
- Objective & Strategy (Mar 12)
- Research (Mar 15)
- Data Analysis (Mar 17)
- Conclusion (Mar 25)
- End of Project (Mar 30)
- + Add a card

## References

- 1Password. (n.d.). *1Password - Password Manager for Families, Businesses, Teams* / *1Password*. <https://1password.com/>
- 1password 8 ios early access design*. (n.d.). <https://blog.1password.com>.  
<https://blog.1password.com/posts/2022/1password-8-ios-early-access/new-design.jpg>
- 1password app layout*. (n.d.). <https://bgr.com>. <https://bgr.com/wp-content/uploads/2018/07/agilebits-1password-apple.jpeg?resize=1020%2C574&quality=82>
- Analogous colors*. (n.d.). <https://99designs-blog.imgix.net/>. <https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Analogous-3-column.png?auto=format&q=60&fit=max&w=930>
- CMYK color scheme*. (n.d.). <https://www.ndsu.edu/>.  
<https://www.ndsu.edu/pubweb/~rcollins/242photojournalism/subtractivecolor.jpg>
- Color psychology in billboard advertising chart*. (n.d.). <http://www.tastyad.com>.  
<http://www.tastyad.com/wp-content/uploads/2019/12/Color-Psychology-in-Billboard-Advertising-Chart.jpg>
- Color shift RGB vs CMYK*. (n.d.). <https://images.prismic.io/>.  
[https://images.prismic.io/rushordertees-web/MWE0N2Q2OWUtMGRmYS00MmJhLWIwM2ItN2I1ZTkzNDEyMDMy\\_rgb-vs-cmyk-convert.jpg?auto=compress,format&rect=0,0,900,540&w=900&h=540](https://images.prismic.io/rushordertees-web/MWE0N2Q2OWUtMGRmYS00MmJhLWIwM2ItN2I1ZTkzNDEyMDMy_rgb-vs-cmyk-convert.jpg?auto=compress,format&rect=0,0,900,540&w=900&h=540)
- Color wheel example*. (n.d.). <https://static.wixstatic.com>.  
[https://static.wixstatic.com/media/fd6093\\_7ee5353eec4940518c91ebd5c4bdaa69~mv2.jp](https://static.wixstatic.com/media/fd6093_7ee5353eec4940518c91ebd5c4bdaa69~mv2.jp)

g/v1/fill/w\_640,h\_480,al\_c,q\_80,usm\_0.66\_1.00\_0.01,enc\_auto/fd6093\_7ee5353eec4940  
518c91ebd5c4bdaa69~mv2.jpg

*Complementary colors.* (n.d.). <https://99designs-blog.imgix.net/>. <https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Complementary-3-column.png?auto=format&q=60&fit=max&w=930>

*Cool colors in color wheel.* (n.d.). <https://99designs-blog.imgix.net/>. <https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Cool-colors-2-column.png?auto=format&q=60&fit=max&w=930>

Decker, K. (2022, December 21). *The fundamentals of understanding color theory.* 99designs. <https://99designs.com/blog/tips/the-7-step-guide-to-understanding-color-theory/>

Faverio, M. (2022, January 13). *Share of those 65 and older who are tech users has grown in the past decade.* Pew Research Center. <https://www.pewresearch.org/fact-tank/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade/>

*Inspiration image nav bars.* (n.d.). <https://i.pinimg.com>. <https://i.pinimg.com/564x/9b/23/63/9b236381a00a7e69bfcecee296f235e4.jpg>

LastPass. (n.d.). *#1 Password Manager & Vault App with Single-Sign On & MFA Solutions / LastPass.* <https://www.lastpass.com/>

*Mobile device orientations.* (n.d.). <https://www.geonetric.com>. <https://www.geonetric.com/wp-content/uploads/Hand-holding-smartphone-370x246.jpg>

*Mobile device thumb reachability.* (n.d.). <https://miro.medium.com>. [https://miro.medium.com/v2/resize:fit:948/0\\*LGs-zf1C4Ht4svsF.png](https://miro.medium.com/v2/resize:fit:948/0*LGs-zf1C4Ht4svsF.png)

Pew Research Center. (2022, December 14). *U.S. Surveys* / *Pew Research Center*.

<https://www.pewresearch.org/our-methods/u-s-surveys/>

*Tech use by age methodology topline*. (2020). Pew Research Center. Retrieved March 26, 2023,

from [https://www.pewresearch.org/wp-content/uploads/2022/01/Tech-use-by-age-](https://www.pewresearch.org/wp-content/uploads/2022/01/Tech-use-by-age-Methodology-Topline.pdf)

[Methodology-Topline.pdf](https://www.pewresearch.org/wp-content/uploads/2022/01/Tech-use-by-age-Methodology-Topline.pdf)

*Triadic colors*. (n.d.). <https://99designs-blog.imgix.net/>. [https://99designs-](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Triadic-3-column.png?auto=format&q=60&fit=max&w=930)

[blog.imgix.net/blog/wp-content/uploads/2017/02/Triadic-3-](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Triadic-3-column.png?auto=format&q=60&fit=max&w=930)

[column.png?auto=format&q=60&fit=max&w=930](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Triadic-3-column.png?auto=format&q=60&fit=max&w=930)

Vojinovic, I., & Vojinovic, I. (2023, January 20). *Save Your Data with These Empowering*

*Password Statistics*. Dataprot. <https://dataprot.net/statistics/password-statistics/>

*Warm colors in color wheel*. (n.d.). <https://99designs-blog.imgix.net/>. [https://99designs-](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Warm-colors-2-column.png?auto=format&q=60&fit=max&w=930)

[blog.imgix.net/blog/wp-content/uploads/2017/02/Warm-colors-2-](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Warm-colors-2-column.png?auto=format&q=60&fit=max&w=930)

[column.png?auto=format&q=60&fit=max&w=930](https://99designs-blog.imgix.net/blog/wp-content/uploads/2017/02/Warm-colors-2-column.png?auto=format&q=60&fit=max&w=930)

*Why Color Matters*. (n.d.). Colorcom. [https://www.colorcom.com/research/why-color-](https://www.colorcom.com/research/why-color-matters#:~:text=2.,is%20based%20on%20color%20alone)

[matters#:~:text=2.,is%20based%20on%20color%20alone](https://www.colorcom.com/research/why-color-matters#:~:text=2.,is%20based%20on%20color%20alone)

Yang, J., & Shen, X. (2022). The Application of Color Psychology in Community Health

Environment Design. *Journal of Environmental and Public Health*, 2022, 1–10.

<https://doi.org/10.1155/2022/7259595>