LUDWIG MAXIMILIAN UNIVERSITY OF MUNICH
Munich School of Management and
The Institute for Informatics
Master of Science in Media, Management and Digital Technologies

Master Thesis

Investigating User Behaviour and Security During Online Payment Using Mouse Movement and Gaze Tracking

Kai Man Wong

Kai.Wong@campus.lmu.de

Time allowed for completion:	31. 8. 2021 to 01. 3. 2022
Supervisor:	Felix Dietz
Examiner:	Prof. Dr. Florian Alt

Abstract

Due to the growth of online shopping behavior, online security concerns, and easy-to-access eye gaze and mouse-tracking technology, we can form a new way to investigate how users interact with a system requiring a high-security level. This study helped to understand the fundamental differences between eye gaze, mouse data, and other user authentication methods. Based on the results of literate research and experiment results, the study suggested a flexible schema to apply eye gaze tracking at different levels to develop a system that adds value to them instead of adding extra cognitive load during the authentication process.

Acknowledgements

I would like to thank my supervisors, Felix Dietz and Prof. Dr. Florian Alt, for providing invaluable support, feedback, and space for experimenting with new ideas during this thesis research process.

I have learned the valuable skills and methodology to test the hypothesis with a tangible result and research a new topic that would continue being advanced and applied to society.

Task Description

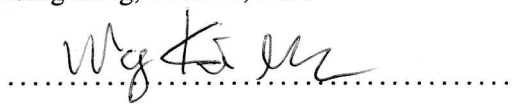
Build a website, which contains the component of a web client, and includes the mouse tracking and eye gaze tracking components. This study aims to study and collect users' mouse and gaze movement while doing online shopping activities at a web store client.

Tasks:

- Conduct a literature review
- Design and implement a web-based online shopping site for participants of the experiment to browse products and interact with the shopping site
- Conduct the user study and collect data
- Conduct the analysis on the received data and the study process
- Report the results from the analysed data and reflection on the study

I hereby declare that I have completed this thesis independently, that I have marked all quotations as such and that I have indicated all sources and aids used.

Hong Kong, March 1, 2022



Task Description

Build a website, which contains the component of a web client, and includes the mouse tracking and eye gaze tracking components. This study aims to study and collect users' mouse and gaze movement while doing online shopping activities at a web store client.

Tasks:

- Conduct a literature review
- Design and implement a web-based online shopping site for participants of the experiment to browse products and interact with the shopping site
- Conduct the user study and collect data
- Conduct the analysis on the received data and the study process
- Report the results from the analysed data and reflection on the study

I hereby declare that I have completed this thesis independently, that I have marked all quotations as such and that I have indicated all sources and aids used.

Hong Kong, March 1, 2022

. . . . . .

Contents

1 introduction

1.1 Background

Due to the increasing number of online payment activities, more security threats are associated with online payments. Mouse tracking is already an established tool in several fields, while eye gaze tracking has become increasingly convenient since cameras are pre-installed on our laptops or mobile phones. It would be interesting to investigate the combined topics of online security, mouse tracking, and eye gaze tracking to enhance security during online payments.

[KAR+20] summarized the role of eye gaze in security and privacy applications and gave a classification of its utility, which is to authentication, privacy protection, and improving security based on gaze behavior. It also provided Humanâcomputer interaction (HCI) with eight directions on eye gaze tracking and challenges regarding it. The paper is based on these suggested research directions. The research direction of this paper will explore all three utility areas suggested by it and add mouse tracking in concern.

1.2 Motivation

Since mouse trackers have been used for a long time, and web cameras are almost ubiquitous, this study can reveal the user's mental activity by combining the two methods. Additionally, the study also concerned about online payments, which have become a significant security issues. With the ability to track a person's gaze and mouse, it provides an insight into their perspective while doing online activities.

We hope to use the study to know how users behave and how the use of mouse and eye gaze tracking can be implemented onto the system as a fundamental way to enhance the security or as the extra level of security that is adjustable according to the user's need.

The insight from the study can be applied to both online payment and online shopping scenarios, as both activities are hard to be separated. The online payment activities are brought mainly by the online shopping events or other types of purchases activities online. We would want to investigate the typical moment of an online shopping or payment activity, which would involve the registration, purchasing, login, and payment process. These steps of an online shopping activity would provide a lot of valuable insights and behavioral patterns that could be used to analyze the users and help authenticate them.

However, to develop a safe system that the public would adopt, users' experience and usability are also concerned. Thus, the investigation concerning the user's interaction experience would need to be measured not just on the data point but also by their opinions.

2 Theoretical Background

To understand the topic, the fields related to mouse tracking, eye gaze tracking, user behavior concerning shopping online and payments, and the secured interface design need to be explored and presented here.

2.1 Online Shopping Activity

An online shopping behavior as the process of purchasing products or services over the Internet [LL00]. Similar to traditional shopping, online shopping involves five steps. It is found that shopping offline is not always safer than shopping online. The current mechanism of some online shopping makes it a safer option than shopping offline. As mentioned in a study, online shopping is a complex process, where consumers perform a lot of activities, including performing the payment, picking up the goods, and confirming the receiver's information [Hao12]. As a result, there is a high chance that the information will be exposed during the process. Also, the researchers come up with three pillars defining a cyber security program that considers technology, process, and people [LAS13]. The application of mouse tracking and eye gaze tracking can enhance the security of these three perspectives.

2.1.1 Top online shopping concern

A study found that when the consumer compare between two different websites, they tend to purchase the product depending on the price, even when it requires more comprehensive data disclosure [JPH12]. It shows that price is still at the concern, even security preventing people from shopping online.

2.1.2 The mechanism for ensuring the safety of data transmission

The online transactions can be secured with HTTPS and SSL certificates and extra security provided by the Extended Validation (EV) certificate. HTTPS stands for HyperText Transfer Protocol Secure, which is secured via Transport Layer Security protocol (TLS). It provides encryption, data integrity, and authentication layers to protect the data sent between the user's computer and the site [goo22]. The SSL certificates, can warn users about a variety of certificates, for example, when the server's certificate has expired, mismatches the address of the server, or is signed by an unrecognized authority [SEA+09]. Another way to authenticate a web page is through an EV certificate, which certifies whether it belongs to a legally recognized corporate entity. In FF3 and IE7, the address bar of a website with such an owner is shown in green, and the name is also displayed.

2.1.3 The failure of safety measures in data transmission

A study found that half of the participants could not identify a secure browser connection [BJM09]. Also, by using eye-movement tracking, a study found that participants paid no attention to web browser security cues, e.g., the SSL icons. After priming, 69% of participants notice the lock icon after being on the lookout for security information [WI05]. It is also found that even removing the SSL indicators from a banking website. All participants still provided their passwords [SDOF07]. A study pointed out the reason why the HTTPS is failed to be implemented because the participants ignored the browser's address bar and status bar and the security indicators [DTH]. Only about a third of our participants had noticed this text indicating Hypertext Transfer Protocol over Secure Socket Layer or Transport Layer Security. Some who reported having noticed both "HTTP" and "HTTPS" did not think that the "s" indicated anything [BVOP+09] [SEA+09].

2.2 Usable Security Interface

2.3 How human process and perceive information

Researchers found that warnings are more effective if they give the instructions on how to avoid the hazard and indication of the potential severity of the consequence if the hazard is not avoided [RLR00] [WGF+87]. However, to design a security system, the obvious of the warning signal is not always the best. The researchers also study the security indicators that can effectively motivate users to search for them and understand their usefulness. However, designing a security indicator with an obtrusive design also causes the users to ignore them, as it may cause them to be annoyed or too accustomed to it [SBVOP08].

Research has found that warnings must be noticeable, legible, understandable, memorable, believable, and motivating in order to facilitate comprehension and compliance. They described a possible model for processing warnings. The principles can be applied to other risk disclosures such as informed consent forms, credit card terms, and software licenses [Wog18].

2.4 Behavioral data tracking

The mouse cursor can be used as an indicator to measure habituation on a participant's part regarding how they interact with the computer and it serves as an effective way to develop a warning system based on these data [AVK+16] .

In psychology, cognitive science and applied research areas, eye gaze tracking has been used for many years to make inferences about perception, cognition and brain function[Duc02] , [Ray98]. Security applications were among the early adopters of eye gaze tracking.Initially, biometric authentication and gaze-based password entry were the focus of early research. Various applications of eye tracking have been developed since then katsini2020role.

2.4.1 Types of Eye Movement

The study on eye movement field has defined the definition and how to assess the fixations and saccades [HNN+18].

Fixations are often defined as pauses of at least 100 ms, typically between 200 and 600 ms. We only see a relatively narrow area of the visual scene with high acuity during any one fixation [MB14].

Saccades are the rapid eye movement that the eye that moves the fovea rapidly from one point of interest to another. that scan the area to perceive the visual scene accurately [MB14]. Saccades are quick, ballistic jumps of 2 degrees or longer that take about 30 to 120 ms each [FB95].

Smooth pursuit movement is when the eyes move smoothly following a moving target [MB14].

3 Previous Work

3.1 Eye gaze tracking studies

The researchers have been using area of interest (AOI) to analyze eye gaze behavior. It involves selecting specific areas of the visible stimulus, then extracting metrics for those areas. The typical AOI includes the header, the body and the bottom part of a web site. Additionally, first fixation (TTFF) is calculated, which measures how long it takes the respondent to look at a particular AOI from the stimulus[PUM19]. The time spent: quantifies how long respondents spent viewing a particular AOI. Based on the ratio, the researchers can see how many of your respondents focused their gaze on a specific area of interest (AOI).

3.2 Privacy and condition terms

The eye tracker can be used to measure the way you consume privacy terms online. The basic duration time is used to explore how participants have interacted with policy. Results indicate which paragraphs were read and fixed on most, relative to their size, suggesting what information participants found more important or relevant to them in the text- particularly those concerning the kinds of data collected and how it is used by the researcher [Ste16].

The consequences of not reading privacy policies, however, can be severe. When a user is unaware of the terms of her engagement with a company, she may unknowingly consent to certain uses of personal information she disapproves of. The findings also indicate that when a website's privacy policy is automatically presented to users, they are likely to spend more time reading it. If a user is given the option of accepting the website terms and conditions without reading a policy, they will usually skip reading it. Even when they choose to click on a link that is not mandatory to read the policy, they spend less time reading it. According to the study, only one-fifth of the participants clicked on the link to read the policy and those who did skim through the text. Additionally, the study shows that participants had a better understanding of their rights and restrictions on the use of personal data collected during the experiment and that enhance the perceived safety of using the system [Ste16].

3.3 User's attitude toward privacy policies

The researcher used eye-tracking to explore usersâ attitudes towards privacy policies. They revealed usersâ tendency to read the policy when presented by default, while when given the option to sign their agreement without reading the policy, they tend to skip it, but participants who actively choose to read the policy spend significantly less time and effort on reading it than participants in the default condition [Ste16].

4 Concept And Implementation

4.1 Problem Formulation

By collecting partial eye gaze tracking and mouse data, with the geographical, quantitative, and open-ended questions to the users, we want to find if particular patterns would be an essential focus to discuss its implication. Moreover, with literature research on the application and mechanism of eye-tracking, how can it be combined in an interactive website to further study users' online payment behavior or create a more secured system, based on the discovery we have.

4.1.1 Research Question 1

Which mouse and eye gaze behaviors are particularly important at different stages of the study and can we find patterns in these data? The investigation would focus on registration/login, browsing products, and processing payments.

4.1.2 Research Question 2

Do users pay attention to the hints and cues to determine if a website is safe during security-critical situations? It is done by investigating if they look at the privacy terms, membership terms, and payment security indicators.

4.1.3 Research Question 3

Can we develop an eye-tracking and mouse tracking system that can allow us to identify the users, in security-sensitive situations, by analyzing the data within the scope of particular participants?

4.2 Shopping Site Client

An interface that mimics a typical online shopping experience will need to be implemented to investigate the user's behavior during online payment. We researched how a typical online payment procedure would be by taking reference of online stores, including Zara Home [Hom], HM [HM], IKEA [Ger], MADE [Mad], and MyConcept Hong Kong [MyC]. The online shopping interface is chosen to be a furniture store to reduce gender bias. In such a setting, both females and males could choose the same set of products. The products displayed in the interface are also designed to be gender-neutral.

In the conception phase, the shopping experience was designed to be two sessions and designed in a way that the behavioral data of users during the first time and second time interacting with the web interface can be analyzed so that the system can decide if the user of both sessions is the identical person. This can provide an additional authentication method, apart from username and password authentication. This concept is useful when the users want to have extra authenticating, for example, when they want to have the password, SMS, and their behavioral tracker activated at the system, to prevent other people from fraudulent use of their account.

To be compatible to track the user's behavioral data, the client's user interface needs to include the component of a mouse tracker and eye tracker. Also, most elements, including buttons, images, and information displayed, will add the hovering and click tracker.

After researching, it was decided that a landing page, a user authentication (i.e., registration and login system), the product browsing phrase, and the payment process would be needed to simulate a typical online payment experience.

1	Availability
2	Product name
3	Product number
4	Original price
5	Number of people already brought the product
6	Rating from other buyers
7	Warranty
8	Color
9	Height
10	Width
11	Depth
12	Weight
13	Other details
14	Return information
15	Delivery time

Table 4.1: The information displayed on the product browsing page.

4.2.1 Landing Page

The landing page, which is often the first page that the user interacts with the site, is created to mimic a typical online shopping site. The users can find part of the information they need to shop for the targeted products. There are eye-catching banners that provide sales details and a quick glance that introduce the online store to the user. This page can also detect how the users decide to finish the task – to shop through this page or the navigation bar.

4.2.2 Registration/ Login

In order to authenticate the users for more than one session to record their behavioral data, the users are requested to register and log in to the system before the checkout process. They are required to fill in a form with required fields, including the first name, last name, email address, and password to register an account. They can choose to provide their birthday to receive the offer and check a box to subscribe to the newsletter from the website. Before clicking the "Register Now" button, there are the membership terms and conditions and privacy policy, which are already partially displayed so that the users have the option to continue scrolling to read it or to ignore it. A tracker of how much the users have scrolled is added here.

4.2.3 Product browsing

At the web store client, there are five pages to display a total of 118 products for the users to shop. The five pages are the Sale, New In, Living Room, Bedroom, and Decoration page. Each page follows the same design, which displays four items in each row, and there are two items at the end of the row. Users can click the thumbnail at these pages to enter a product page dedicated to a single product. On each product page, the following product details are given:

4.2.4 Payment

To go through the payment page, users will need to go to the shopping cart to view their chosen items and click the "proceed to checkout" button. Then they will go to the checkout form, in which they are required to put their shipping address and phone number. After clicking the "continue" button, they will land to the final stage of an online payment – to fill in the payment details. The

option of paying by credit card is provided on the payment page. The users need to put down the credit number provided at the beginning of the study, which is the same for every user. A service condition term is displayed under the "pay now" button, which is partially displayed, and users can scroll to view it. A tracker onto the service condition window scroll is added here.

4.2.5 Membership Terms and Privacy Terms

The membership and privacy terms are shown on the registration and payment page. We want to detect if the users have paid attention to it. According to a study, only one-fifth of the users read the privacy terms, and when users have clicked the terms to read it by choice, they tend to skim through it quickly[Ste16]). In our study setting, the terms are presented partially to remind the users that they exist, but users can also choose to scroll through it as an active choice to continue reading it. However, the terms are more notable in our setting than the typical online shopping sites because they do not need users' extra effort to open them.

The membership term defines the rights of both the company and the customer for using membership services and products provided by joining the membership programme and how disputes will be resolved. It also mentioned under which situation the company can terminate the membership, and the customer has the right to complain to the European Union's online dispute resolution portal (ODR platform).

The privacy terms are formed according to the General Data Protection Regulation (GDPR) to inform the users about how the company collects, uses, processes, and stores their customer's data. They explain why they own the data and the examples of the data. It also mentions the users' rights, such as requesting to check what information is stored, erasing them from the company, and the exception when the data cannot be erased. The company's address, taxation number, and the contact detail of the data protection officer are also provided inside the terms.

4.3 Shopping Site Task

In order to create a data collection environment where we can collect enough behavioral data, and users' behavioral data collected need to be comparable between themselves and to other users, the tasks are specified instead of providing a free shopping experience. So in our case, in the study, users need to follow the guideline on which items to buy. This is different from a typical online shopping situation when users have the goal of shopping target in mind; here, we provide the shopping target from our side.

However, the task does not include using the user's memory load because we provide hints on what items they would need to look for at the top-right side of the shopping site.

The shopping tasks are tested until they reach the level that it is feasible to do, and with a bit challenging, users need to compare between different products and ensure they would go through the three main product category pages in the living room bedroom and decoration page. By clicking, open the product page, compare between products, and target their attention to look for specific information position.

4.4 Implementation

In order to let participants access the web store experience despite their location, choice of desktop or laptop computer, browsers, the web-store need to be able to access online and compatible for

users with a different way of accessing it, which allows us to add on the tracker and authentication system.

After finding the currently available platforms, e.g., the online web store platform, we discovered it would be restricted to what components to add and affect the functionality. Therefore we built our website and added the two external APIs for the shopping cart function and eye-tracking, plus the instruction page and survey, which are not tracked with behavioral data.

4.4.1 Technical Concepts

The implementation structure followed the traditional client-server models. The web store was created as a web app, accessible from the internet as a web page. A web server was created to host the web app and collect the data, including the user's login details, their behavioral data, and survey data. The React JavaScript Framework was chosen to create the web app, as it offers many utilities and libraries to create the web interfaces, JavaScript functionality to access the tracer's library online, and the shopping cart library, which is provided from external as API.

The implementation of the server and tracker functionality and the handling of the storage of the tracker data in the study was assisted by the help of a student from the Usable Security and Privacy Group at the Research Institute for Cyber Defence and the University of Bundeswehr Munich.

The Node.js run time environment is chosen to write the server-side code because it provides an efficient non-blocking I/O model, which can handle data-intensive real-time applications with a single server [Fou22]. It is suitable for our study in which the mouse and eye gaze data need to be constantly tracked and sent to the server. The Express library is used to create a web server, which provides a thin layer of web application framework that is efficient to handle the HTTP request and error handling that uses JavaScript [Sc17]. In our project, only handling the text data is needed. Therefore, the efficient Express is used.

The Cascading Style Sheets (CSS) were used to structure the web store so that the styling is consistent on different pages and can be reused to ensure all the products are presented in the same styling.

4.4.2 Client

The client web store was created using the React JavaScript library, which efficiently creates interactive user interfaces. It will update and render the component when the data changes [MP22]. This is useful; when the user has logged in, the state will change, and the corresponding elements will match the current state. Also, the items will be deleted or refreshed in the shopping cart when users have interacted with the component. Here the state of the shopping cart products, sessions of the user, the user ID is essential, as they have been used throughout different stages of the programme.

Additionally, components can contain other components. Data is passed from one component to another is called props. Here, the product is the critical component that we have applied the component principle. The template of the display of the product is reused for the five pages (for the New In, Sale, Main, Living Room, Bedroom, and Decoration). The function of the reusable component has avoided the repetition of creating the exact product displaying a page for the 118 products to display the same format on every page. The components return code in JavaScript Syntax Extension (JSX).

Add the library of commerce.js for the shopping cart function, and create our database for the products. This granted the maximum control over the interface, with eternal API for the eye gaze tracking and the mouse tracker component that we implement using the function provided at the browser. We also used the Commer.JS library provided by the third party, which created the call for the product function and provided functionality when users have clicked to add to the shopping cart, and we modify the programme to include our database.

The website client contains the five pages, main page, registration, shopping cart, checkout, payment, and tracker. The "tracker" component is placed as the highest component, and it is activated once the user has clicked the continue after the instruction page. With the clicking of the button, the tracker, with the ID assigned to each user, is activated.

We did not limit the display size of the website in order to mimic the realistic shopping experience, as in real life, users may also adjust the web browser to their computer screen size, and for an eye tracker and mouse tracker functionality, it is expected to track despite the fact that the user's opened web browser size. However, to ensure we can know the relative position that their mouse and eye gaze are, the process of transforming the tracked behavioral data position is needed to be done at the client-side and sent to the server.

Moreover, it is called a JavaScript "setInterval" function to activate the tracking process. In every 33 milliseconds intervals, the data is captured once and logged into the user's data entry. Every five seconds, the array was sent to the server using the HTTP POST method.

The mouse and eye-gaze coordinates were transformed at the client's side so that the coordinates can be evaluated later, which eliminates the factor of the participant's screen size and adds the scrolling amount of the user. The returned transformed x and transformed y coordinates are relative to the top left of the corner of the email interface so that we can analyze using the same baseline later in the analysis.

Data ID	Data Name	Data Description
1	Time stamp	The time of the data being taken in the format of a time stamp
2	User ID	An unique user ID is assigned randomly to record them at the database
3	Current Email	An unique email address as the login credential that the user created at the registration page
4	Current password	An unique password that the user created at the registration page
5	Margin to screen (Left)	The value of the gap between of the user's inner window left to the browser windows left edge
6	Margin to screen (Top)	The value of the gap between the user's inner window top to the browser windows top edge
7	Plain Mouse position X	The horizontal position of the user's mouse with browser's top left corner as origin point
8	Plain Mouse position Y	The vertical position of the user's mouse with browser's top left corner as origin point
9	Transformed mouse position X	The horizontal position of the user's mouse with web store's top left corner as origin point
10	Transformed mouse position Y	The vertical position of the user's mouse with web store's top left corner as origin point
11	Browser width	The width of the browser window
12	Browser height	The height of the browser window
13	Page scroll X	The amount of the page scrolled horizontally
14	Page scroll Y	The amount of the page scrolled vertically
15	Eye gaze position X	The horizontal position of user's eye gaze position with browser's top left corner as origin point
16	Eye gaze position Y	The vertical position of user's eye gaze position with browser's top left corner as origin point
17	Eye gaze shifted position X	The horizontal position of user's eye gaze position with web store's top left corner as origin point
18	Eye gaze shifted position Y	The vertical position of user's eye gaze position with web store's top left corner as origin point
19	Head position X	The horizontal head position of the user
20	Head position Y	The vertical head position of the user
21	Head position Z	The head position of the user on the Z-axis
22	Head position Yaw	The yaw movement of the head (i.e., the left and right direction).
23	Head position Pitch	The pitch movement of the head (i.e., the up and down direction)
24	Head position Roll	The roll movement of the head (i.e., the tilt)
25	Hover Events	The hover event(s) the user activated at the current moment
26	Click Events	The click event(s) the user triggered at the current moment
27	Mouse click position X	The horizontal mouse click position with browser's top left corner as origin point
28	Mouse click position Y	The vertical mouse click position with browser's top left corner as origin point
29	Membership term scroll	The scroll value of users performed at the membership term window
30	Privacy term scroll	The scroll value of users performed at the privacy term window
31	Start time	The moment when the user has activated the tracker.

4.4.3 Back-end

A web server was created using the NodeJS framework "Express" [insert express citation here]. The web server hosted the entire web app and was connected to a PostgreSQL database. For this study, because the data for the user's credentials, behaviors, and products are not extensive, it is saved as the text file to be transferred between the client and the server. The database is also included at the server, which can be accessed via an SSH connection to retrieve the user's data and survey response in real-time. The files that are included in the database includes:

Logged data: user's unique identification data, mouse and gaze data

Login credential: Email address, password, first name, last name and a salt value

Post accuracy data: Accuracy data of users after completing the interaction with the web store client

Survey data: User's geographical data and survey responses

4.4.4 Products Creation

The photos that create the products are from the Pixels License. The attribution is not required, and users can modify and edit them as they like. Moreover, users cannot sell the products on a poster, print without modifying it [Pex]. Furthermore, the photos are created via the online photo editing site, Canva, and the permitted uses of content used to permit to do, for school or university projects [Can21].

To investigate users' behavior when interacting with an online shopping site, a website displaying 114 products is displayed. In each section of a product category (living room, bedroom, and decoration page), 38 products are displayed. Check whether the user is in the first session or the second session is created.

In each session, six products out of the 38 products in each product category were provided, offering a 15.80% chance the to the expected at the instruction. In total, 18 products out of the 114 products were available for the users to choose from. However, the finishing of the session doesn't limit them to choosing only the target 18 products. Users can also shop for products outside the suggestion on the instruction page.

5 User Study

5.1 Study Design

We performed an online shopping study (n= 12) using the design that we mentioned at the concept and implementation (see Chapter 4) that consist of a survey at the session to measure the user's geographical details, online shopping habits, response to the eye-tracking experience, and their opinions regarding the usage of mouse tracking and eye gaze tracking to enhance online shopping site's security.

5.2 Participants

Participants were recruited via a university mailing list, social media, messenger groups, and personal contacts. Because the experiment is allowed to be completed at participants' desired time online, some did not complete the second session or survey before the experiment closed. As a result, 12 participants (4 females, 8 males) are validated in the study. Participants have to fulfill the requirement of wearing no glasses or using contact lenses to participate in the study. The average age was reported at 24.5 years (SD=3.92, range=19-32). Our participants were mostly students or teachers from Germany or Hong Kong. The set of other participants' professionals also included a cyber security consultant and a contact tracking coordinator. 6 participants have reported experience with using eye-tracking, 2 have little experience, while 4 reported they do not perceive they have experience with eye-tracking. They were either given a 5 Euro value of Amazon voucher or credits for the informatic student in completing experiments.

5.3 Procedures

Each participant was asked to use their desktop or laptop with permission to access their webcam to open a link that directed them to the study website. They receive a brief message through an email or a social media contact. The message mentioned the theme, reason, and institute which conducted the study. The study was designed according to the concept of providing authentication by the behavioral data of the users of two sessions initially, where the users are asked to perform similar tasks for both sessions. Due to the time limit and technical limit, the first session with survey data is collected.

5.3.1 Requirement and Consent

When the user is at the website of the study, the instruction page is presented at first to ensure that the participants fulfill the following requirements to be able to continue the study:

- Having a minimum age of 18
- Do not wear glasses (if possible, use contact lenses)
- Completing 2 sessions of the study. The second session can be done 12 hours after the first session. Using a laptop or desktop computer with a decent webcam Allowing camera access for this website. Accessing the website only Google Chrome or Firefox Having a good lighting without strong light behind you Having a pen and a piece of paper or a phone to record the credit card information
- Writing down the Email address and passwords you created this session for the second session

Then the introduction on how the system work is presented to make sure the participants complete the study without discontinuity, such as to maintain the largest window size for browsing the website, not using the refreshing function, go back button (apart from during the product browsing process) or auto-fill function. After that, a consent form is presented, which mentions the data collection purposes, how the participants could request the data we collected, and whom they can contact. This information complies with the General Data Protection Regulation (GDPR), and the participants have to agree on it before starting the study.

5.3.2 Task Instruction

The following task instruction is provided:

"You have just rented an empty apartment with no furniture. Your friend just shopped some pieces of furniture at the online furniture store "DigitFurns." and recommended you to shop there too, because the quality of the products and the service were good. You compared the price with other stores and found that the price is reasonable and with free delivery, so you decided to shop there."

A picture of the empty flat was shown. This setting eliminates the factors that affect the participants (e.g., the website's trustworthiness) and ensures the participants have a similar reason to shop.

The participants are asked to shop for three items:

- a sofa with a depth less than or equal to 85 cm
- a chest of drawers with a width more than or equal to 80 cm
- a table lamp with a wattage more than or equal to 75W

However, they do not need to remember the details of the items as they will appear as a hint box later in the experiment. Also, they can shop for other items they want. In order to simulate a credit card input behavior, where users look at information from a physical card and transfer it into the input box of a credit card input session at the website, a demo credit card is given, and participants are asked to drop down the credit card information.

5.3.3 Webcam Calibration

The calibration process started after they had clicked the "start" button. The process included a nine-point calibration and a head movement calibration. This process took about two to three minutes. After the completion of the calibration, the users are directed to the main page of the website.

5.3.4 Registration, Shopping and Payment

Users could either begin by shopping for the products or register during the study. They would need to register an account before the checkout process because there is a validation if they have logged in at the checkout page.

The shopping task would require them to browse the products in each category several times before finding the one according to the instruction. They would either use the category button at the navigation bar or use the back to previous page button from their web browser, causing the

product page to be the page the user interacts with the most.

This process simulates a typical online shopping experience, where they are introduced to the main page, providing the sale and discount code for a website, and guiding them to the information communicated by the store owner. They would need to open an account and use the credit card as the payment method. The system does not check the products they chose; therefore, users may have chosen the wrong products at the submission of the experiment.

5.3.5 Post Study Calibration Accuracy Test

The users took a nine-point accuracy test after receiving the confirmation that their tasks were completed. Afterward, they were continued with the post-study survey.

5.3.6 Post Study Survey

The post-study survey included demographic information, such as gender, age, profession, devices used by the participant for online shopping, and the frequency they shop online. Also, the participants were asked to rate their agreement with ten presented statements on a five-point Likert scale (1= completely disagree, 5=completely agrees). The following topics are measured:

- self-perceived level of expertise with security, computer and eye-tracking
- the usefulness of the security features at the website
- the perception on adding eye gaze and mouse gaze tracking to enhance shopping security

5.4 Data collection and features

5.4.1 Device specified data

Due to the study not limiting the device resolution to access the study online, various device sizes are collected in terms of their browser width and size. The pixels of the browser's left and top to their computer screen are also collected.

5.4.2 Eye Gaze Data

The eye gaze data are collected beginning from the main page, where the user firstly interacts with the website. Furthermore, according to how long the user interacts when the eye gaze tracker is activated, part of the eye gaze data on the product browsing page is recorded. The data are collected where the users look at the screen represented by X- and Y- position. The transformed Y-position adds the scroll value of the users at their computer at the client-side before sending it to the server. Following features were calculated and observed to analyze eye movements of the users:

- Level of interaction with the area of interest (AOI) in the website's main page: This divided the users into looking at only the first banner without scrolling, scrolling to the middle of the website, or viewing all the promotional banners until the end of the website. The observation is conducted by analyzing the heat map.
- Number of data points that the users look at the web browser's toolbar or address bar: This is measured by counting the data point which the Y-position is in negative, indicating the user's gaze is above and outside the website content.
- Percentage of time spent on the different pages: This is calculated by dividing the data point spent at the current page from the total data point recorded on the website.

- The gaze path the users behave at the main page: This is measured by using the heat map, with a number counting from 1 at each gaze point, to see the path the user created while browsing the web page.

5.4.3 Mouse Data

The mouse data is collected at every page on the web page, with the mouse tracker collecting the X- and Y- positions. The transformed X- and Y-position is also performed at the client-side by adding the scrolling value before returning to the server. The hovering and clicks of the elements are also collected at the website's different pages, in all the buttons and the partial essential visual elements (e.g., the product's picture, the description, and input boxes) that help users decide on the purchase.

The following mouse movement-related features are calculated and observed from the mouse position, hovering and click collected by the mouse tracker, and the heat map:

- Attention spent on the AOI of privacy and security-related information at the registration page: It is measured by the data point spent after the mouse position is at the area between on the acceptance of receiving discount offers by giving out birthday to the clicking of registration button. This area contains the birthday collection terms, membership terms, and privacy terms. The position is measured using the heatmap to check where the point is and calculate the points within the AOI is located. The attention is measured by the percentage of the data point on the AOI divided by the total data point recorded on the registration page.
- Attention spent on the AOI of the security information at the payment page: The attention is measured by how many data points are measured under the credit input field, where the service term for the credit card is provided. It is divided by the total data point measure at the payment page for indicating the level of attention.
- The scroll value of the terms at the registration page and payment page: It is measured by the scroll value provided by a tracker added to the scroll window.

Number of participants access to the website interface	18
Number of validated participants	12
Average age	24.5
Standard deviation (SD) age	3.92
Age range min max	[19,32]
Male number	8
Female number	4

Table 6.1: Demographics of the post study survey

6 Result

6.1 Demographics

For question 5, on which online shopping platform they used, The result has shown that 7 of the participants (58.33%) have used Amazon as the online shopping platform, and other online shopping platforms that they have used include eBay (25%), Zalando (16.67%). Other online shopping platforms they used included Vinte, HKTVmall, Zara, and BestSecret.

For question 6, on the device they use when shopping online, 10 participants (83.33%) have used a laptop as the online shopping device. The second most used device for shopping is the smartphone. 4 participants (33.33%) have used it for shopping online. One participant (8.33%) reported having used a desktop, and one participant (8.33%) reported tablet to shop online.

To answer question 7 on which payment methods the participant used for online payment, 8 used PayPal (66.67%). Secondly, 7 participants have used a credit card as a payment method. Two have used bank transfers (16.67%), one used a debit card, and one used Sofort.

On question 8 on how frequently the participants shop online, 5 participants (41.67%) reported shopping 2 to 3 times per month. Three said once per month (25%), two (16.67%) shop once per week, one shop less than once per quarter, and one reported he does not shop online.

Question 23 asked if the participants found the experiment difficult and for their reasons. 8 participants (66.67%) reported it is not difficult. 4 participants (33.33%) reported it is simple and clear, and three said the instruction on what attributes to find is straightforward. One said the gaming experience had helped him. However, 4 (33.33%) reported difficulty, the reason being without filter to search and not being prepared. However, three (25%) find finding a lamp with high wattage is challenging, regardless of whether they have found the experiment difficult overall.

6.2 The perception of eye-gaze tracking security

Table 6.2 has listed the questions and results on how the participants have perceived their level of expertise with IT security, computer, and feedback on their eye gaze tracking experience. Also, the questions on measuring their willingness to provide eye gaze data for the sake of online shopping security were asked.

The participants have reported a high perceived proficiency at using the computer (M=5, SD=0.67). The self-perceived experience with IT security (M=3.5, SD=1.29) and eye-tracking (M=3.5, SD=1.31) is close to the neutral. However, the level of expertise in IT security and computer knowledge is measured not in detail in this study. A more detailed set of surveys can be

I have experience with IT Security.	M: 3.25, SD: 1.29
I am proficient at using the computer.	M: 5, SD: 0.67
My eyes felt tired after or during the study.	M: 3.5, SD: 1.31
I have experience with using eye tracking.	M: 2, SD: 1.27
At the registration page of the experiment, I used the password suggestion to help my password creation process.	M: 2, SD: 1.27
At the payment stage of the experiment, the privacy term reduced my concern about online transaction safety.	M: 3, SD: 1.38
I am more willing to shop on a website knowing my account is safely protected.	M: 4.5, SD: 0.67
I am more willing to shop on a website knowing my account is safely protected through eye gaze tracking authentication (i.e. the system will alert when it has detected another user is trying to pretend to be me)	M: 2.5, SD: 1.37
I am willing to leave my eye gaze behavioural data (i.e. the record of my eye gaze behaviour while shopping at a website) knowing the company is authorized by me to process my personal information (e.g. the credit card information and the username) already.	M: 2, SD: 1.16
I will shop more often on the same website, knowing that the more I shop, the more accurate the authentication system (to protect my account) will be.	M: 3, SD: 1.22

(M: Median, SD: Standard deviation)

Table 6.2: Result of the Likert scaled questions in the survey

used in future studies.

On question 15, "I am more willing to shop on a website knowing my account is safely protected", most of the participants agree or strongly agree on it (M=4.5, SD=0.67). It showed that the linkage between the willingness to shop on the premise that is the account is safely protected is high.

However, on question 16, "I am more willing to shop on a website knowing my account is safely protected through eye gaze tracking authentication", most people disagree on it (M=2.5, SD=1.37). It showed that the perception of what defines the safe-protected account needs to be further investigated. On question 17, if the participants are willing to leave their eye gaze behavioral data to a company, knowing those companies are already authorized to process their other important personal information, most people disagree with it (M=2, SD= 1.16).

For question 18 on the relationship between shopping more if it increases the accuracy of an authentication system, participants have a neutral response (M=3, SD=1.22).

6.3 Free Text Commentary

Question 20 asked the participant the question on "What usually affects your shopping behavior online?", 5 participants (41.67%) have mentioned the consideration of the product. 4 participants (33.33%) mentioned the consideration of the product includes the product variety, and one mentioned the product quality. The second factor the users (4 participants, 33.33%) response would affect online shopping behavior is the price (or the deal). Other factors are the trustworthiness

of the company, product image, reviews from other customers, corporate social responsibility of the company, online security, necessity to shop online, payment efficiency, social media, shipping speed, convenience, and user experience. One reported on a combination of multiple factors.

Question 21 asked the question on "What aspect(s) makes you feel the online transaction is safe on an online store?". 4 participants (33.33%) reported that the credibility and the authenticity of the website make them feel the online transaction is safe. Three participants (25%) reported the website interface or design. One said, "a professional design gives me more confidence". Two mentioned elements on the web address bar, although they have used different ways to express it. They mentioned it as "the website is secured tag", "green secure site label next to the web address," and "web domain affiliates". Other answers include the reviews, "HTTPS", redirection to the payment website, separate window with encryption is opened. Moreover, one said the website is "safely protected".

Question 22 asked, "Would you like to have eye gaze tracking being used to enhance your account's safety? Why (and why not)?". Half of the participants (50%) reported a negative response. In contrast, three (25%) reported the willingness to try, and three (25%) answered neutrally. 4 participants (33.34%) were concerned about the safety or privacy issue, with two mentioned the worry on accessing the sensitive data on pupil and iris, one mentioned the perception on the unfavorable history on data handling. Those who would try it consider it a novel idea and have positive thoughts on biometric security measures. One considered it being "the safest way to protect a transaction". The neutral responses consider the slow calibration process affecting the online shopping speed, but the participant would consider if the technology is advanced in the future. Two (16.67 %) reported on the lack of knowledge, while one specific it being, they do not know "how well this works and if the eye behavior is that different".

On the last question (question 24), the user are asked about the other opinions regarding eye gaze and mouse tracking and the experience of the experiment. Three participants (25%) gave a positive opinion on the use of eye gaze tracking again. They said "looks interesting", it is "a valuable security measure in the age of increased online risk", it "could be useful," and it is a "new way of making online shopping safe". Opinions on how to decide including eye gaze and mouse tracking by thinking more perspectives are given, such as having consent from the user to activate the security feature, assessing how hard it is for the system being hacked, the acceptance by the public, applying it to a specific area of applications (e.g., crypto wallet or bank account), balancing between the convenience and safety. One mentioned preferring password-based authentication, with the second factor being OTP over SMS than personal attributes.

6.4 Analysis statistical results

The measurement on time spent in the study adapting 1 data point as a unit. Every data entry is a record with the timestamp for analysis. Every data entry is about 33 milliseconds second.

6.4.1 Recorded number of data at different pages

The number of data points records is different for every user, and some spent less time or more time than others overall on the web page. The product page (M=2467.00, 74.01 seconds, SD=1750.56, 52.52 seconds) recorded the most data. Users repeatedly use this website to display various products to perform a similar activity (i.e., comparison of products with the information provided on the page). The second most recorded data is the register page (M=1580.00, 47.40 seconds, SD=1289.19, 38.68 seconds), and the third is the decoration page (M=1312.00, 39.36 seconds, SD=1489.47, 44.68 seconds).

Page Name	Median of No. of data points	Standard deviation of No. of data points
Main	370.50 (11.12 seconds)	160.04 (4.8 seconds)
Register	1580.00 (47.40 seconds)	1289.19 (38.68 seconds)
Product	2467.00 (74.01 seconds)	1750.56 (52.52 seconds)
Payment	994.50 (29.84 seconds)	372.04 (11.16 seconds)
Login	817.50 (24.53 seconds)	901.01 (27.03 seconds)
Living room	823.50 (24.71 seconds)	1394.39 (41.83 seconds)
Bedroom	676.00 (20.28 seconds)	777.70 (23.33 seconds)
Decoration	1312.00 (39.36 seconds)	1489.47 (44.68 seconds)
Cart	302.00 (9.06 seconds)	291.96 (8.76 seconds)
Checkout	1177.50 (35.33 seconds)	970.70 (29.12 seconds)
Sale	296.00 (8.88 seconds)	301.20 (9.04 seconds)
New In	150.00 (4.50 seconds)	339.30 (10.18 seconds)
Confirmation	42.50 (1.28 seconds)	58.86 (1.77 seconds)

Table 6.3: Data point recorded from participants at different pages

Overall, apart from the decoration page and product page, the top three pages that recorded the most data require understanding the information provided by the page and inputting data. Apart from the registration page being one of them, the second is the checkout page (M=1177.50, 35.33 seconds, SD=970.70, 29.12 seconds), and the third is the payment page (M=994.50, 29.84 seconds, SD=372.04, 11.16 seconds).

The amount of data recorded from the users do not have much variance. The data on the confirmation page (M=42.50, 1.28 seconds, SD=58.86, 1.77 seconds) recorded the least amount of data. This page requires only the user to acknowledge receiving the information without much interaction. The page with the second and the third least amount of data is the New In page (M=150.00, 4.50 seconds, SD=339.30, 10.18 seconds) and the Sale page (M=296.00, 8.88 seconds, SD=301.20, 9.04 seconds). The information that appears on these two pages is overlapped with other pages, such as users do not need to seek information at these pages to complete the tasks.

6.4.2 Password Creation

The password field on the registration page has the password requirement of at least eight characters, one digit, one capital letter, one lowercase letter, and a unique character. There are 4 participants (40%) out of the ten who have filled the passwords and fulfilled this requirement. On average, the one who met the password requirement recorded on average 2123 data points (63.69 seconds) on the registration page, and those who did not meet the requirement on average recorded 1924.6 data points (57.74 seconds).

6.4.3 Attention to the security cue at the registration page

Reading the terms of the service, such as security and privacy terms, can enhance the security and right of the users. Only two participants (20%) have read the membership terms on the registration page at the study. Moreover, both of them only read the first term provided by the website, which is the membership term, and ignored the privacy terms.

Average data points of participants who meet the password requirement	2123 data points (63.69 seconds)
SD of data points of participants who meet the password requirement	1668.6 data points (50.06 seconds)
Average data points of participants who do not meet the password requirement	1924.6 data points (57.74 seconds)
SD of data points of participants who do not meet the password requirement	741.5 data points (22.245 seconds)

Table 6.4: Statistic on participants on password creation process

Data points of participant (P5) who read the membership terms	81 data points (2.43 seconds)
Data points of participant (P7) who read the membership terms	558 data points (16.74 seconds)

Table 6.5: Statistic on participants on reading the membership terms

Another area of interest on the registration page is after the user fills out the necessary information and decides if they want to give the optional birthday, the checkbox to tick the receiving offer to email, the display of membership terms, and privacy terms. The data points of those where mouse position is after the birthday input field and before clicking the registration button are used for analysis.

The median on the mouse data in AOI of the privacy and membership-related information (at the location after the birthday input field and before the registration) is 593.5 (17.81 seconds, SD= 305.65, 9.17 seconds). Participant 8 spent the most time on this area of interest (2903 data points, 69.72 seconds), which also is the one who spent the third amount of time on the whole website (18380 data points, 551.4 seconds). However, there is no prominent relationship between how much time the users spent on this personal detail and privacy term area and how much time they spent totally on the website. For example, participant 9, who ranked the 10th at the data record at this AOI (438 data points, 13.14 seconds), spent the second most time on the whole website (19409 data points, 582.27 seconds). The summary on the AOI on the privacy and membership right related information thus is summarized as not depending on the total time spent on the website but of the personal interest in this area.

6.4.4 Attention to the security cue at the payment page

Users could look at several areas during an online transaction to notice if the transaction is safe. Our study measured the attention cue by whether they scrolled the service condition terms and how many data points are recorded when the mouse position belongs to the button to finish the payment. Because if the users have moved the mouse below that button, it indicated they had spent extra effort outside the paying task.

The data has shown that no participants have scrolled the service condition under the payment button at the bottom of the page. The only important data recorded is participant 1, of which 532 data points (15.96 seconds) are recorded at the AOI. Other participants recorded the mouse in this area from 20 to 75 data points (0.6 seconds to 2.25 seconds). There is a positive relationship between the total time spent on the website and the time spent on this area of interest. The top three participants who have spent the most time on this AOI are also the two of the top three participants

who spent the website.

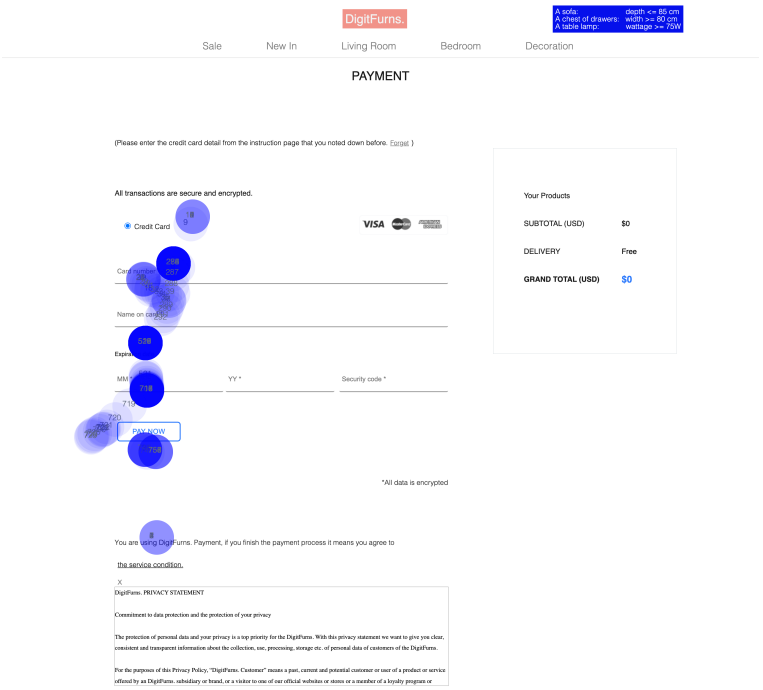


Figure 6.1: Heat map of participant 6 (mouse data)

6.5 Eye gaze data and heat map

Twelve sets of heat maps, made by a scatter plot using either eye gaze tracking or mouse-tracking data, are generated. Each set of the heat map consisted of images and points generated from four pages (i.e., the main page, payment page, product page, and register page). Every heat map on the main page consisted of the eye gaze tracking data and mouse-tracking data. Some of the heat maps on the products page consist of eye gaze tracking data, while some just have mouse-tracking data. This is because eye gaze tracking can be ended at the end of the main page. These four pages are high security-critical pages, as there is the password creation, consent to membership, privacy terms, and credit card payment process. Therefore, the heat map is chosen to be created for these pages.

6.5.1 Behavior at the landing page

The eye gaze behavior with the mouse begins at the main page (i.e., the landing page) is recorded. The behaviors of the participants are divided into three groups – attention remained at the top area (without scrolling), attention to the middle (with scrolling), and acquainted with the information until the end of the landing page (with scrolling).

Most participants (5, 41.67%) scrolled till the end at the main page to see all the options and promotional materials provided on it before moving to the next page (see Figure 6.3). Moreover, 4 participants (33.33%) do not scroll the web page at all, with eye gaze and mouse remains on the upper area of the main page (see Figure 6.1). Three participants (25%) scrolled the page to the middle and, with eye gaze and mouse, focused on the category information provided by the icons (see Figure 6.2).

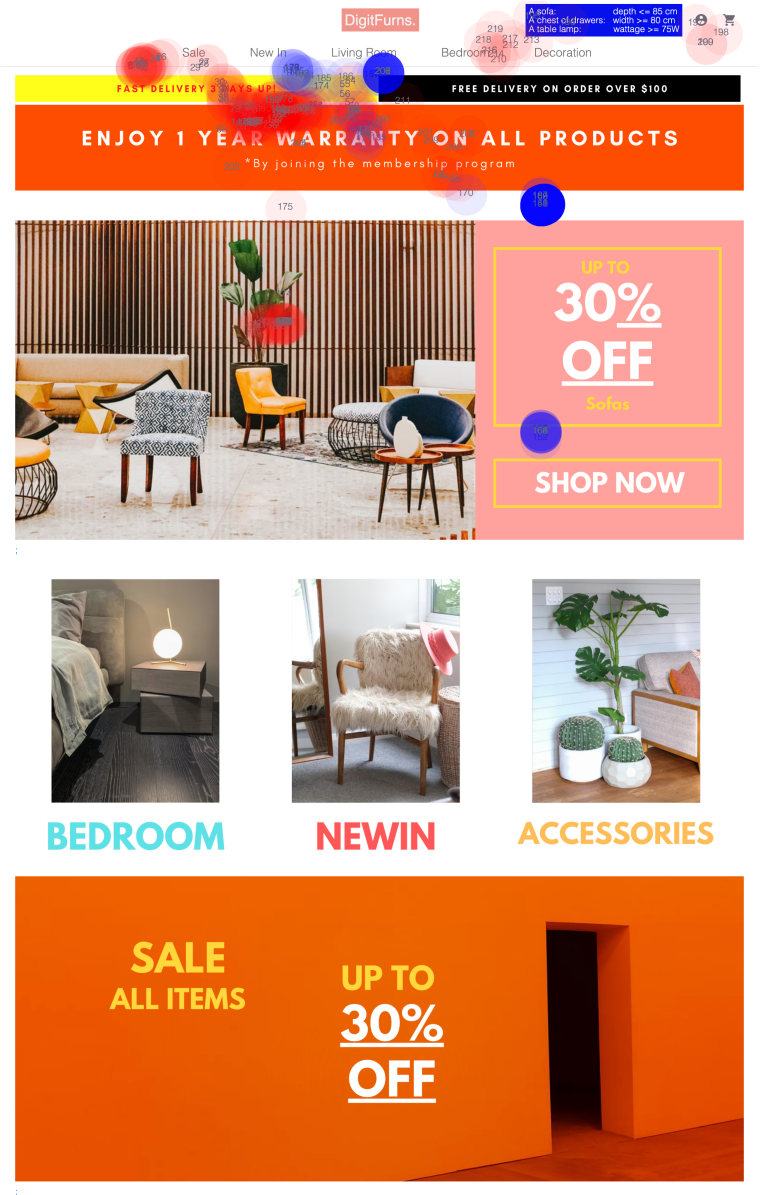


Figure 6.2: Heat map of participant 2 (gaze and mouse reminds at top area without scrolling)

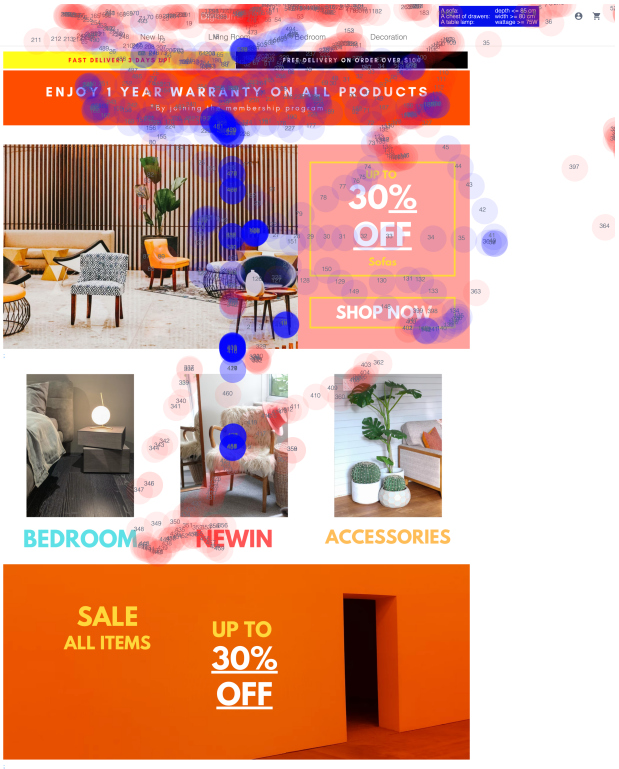


Figure 6.3: Heat map of participant 1 (gaze and mouse to the middle area with scrolling)

6.5.2 Attention on the web browser's tool bar

The attention on the area close to the URL address bar is also analyzed with the heat map and the coordination recorded from the data. Five participants have recorded some eye gaze data points above the web page content area, which indicates they may look at their browser's toolbar or the URL area.

The maximum data points recorded above the web page's content displayed is recorded from participant 1 (170 points, 5.1 seconds), which is 33.60% of the total eye gaze attention recorded. The data points recorded from others users are from 5 to 22 points (from 0.15 to 0.66 seconds), which occupied 2.28% to 7.10% of their eye gaze attention at the main page.

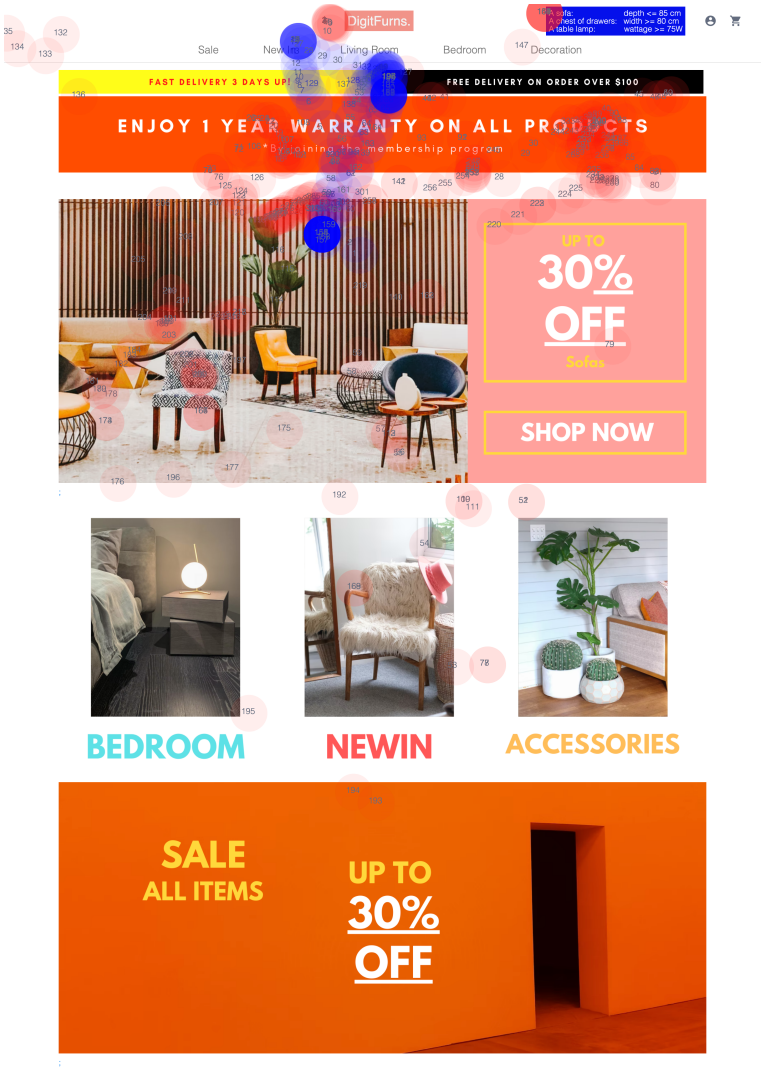


Figure 6.4: Heat map of participant 10 (gaze and mouse reach until the bottom area with scrolling)

7 Discussion

7.1 Limitation and opportunities

7.1.1 Lack of eye gaze tracking data

Due to the limitation of only a short period of the eye gaze data can be recorded, only the main page and part of the products pages can be analyzed. However, it provided a more qualitative and detailed investigation of the main and product pages. The eye gaze data provided, although limited, even reflected on the main page, showed a lot of unseen without it. By mapping the eye gaze and mouse data on the page where the users land, with the ability to choose, and where is always the first page of a web page, we can see that users' behavior is fundamentally different. While although the mouse data are in larger quantity, the difference is smaller than the eye gaze data and the magnitude of how a small snippet of eye gaze data can tell.

In an actual life situation, mouse data collection could be more accepted firstly by the users, and thus it is essential to also design an authentication and security enhancement system with more mouse data. However, the opportunity of having more mouse data on more pages is that we also developed the mechanism to measure the user's attention without the eye gaze data. For example, the area of interest at the privacy terms is measured using the heat map and hovering at the birthday offer information and the registration button.

7.1.2 The necessity of using high level of security measure in shopping website

Although at the result section, the participants share the unwillingness to give their sensitive data (e.g., the behavioral data and they concern about the iris data get lose when associated with the term eye gaze tracking), the study did not investigate on give a setting requires a higher level of security, and that setting is legitimacy and justifiable by user's needing to exchange a higher level of security by their calibration time and the extra effort, and trouble of activating the camera.

7.1.3 Implementation of an embedded eye gaze tracking system

In actual life situations, a system that required the continuity of the eye gaze or mouse tracking required a high level of usability, or careful design, so that the users could go through the calibration process more accessible or do not need to go through calibration at all. There is existing software that can track the eyes without calibration. Thus, the concern of the users forms the result section on the troublesome of the calibration, making them stay neutral toward the technology, which can be affected by a better design of the eye gaze tracking. Moreover, a system that required the eye gaze or being able to use the eye gaze tracking required a user's profile of their eye gaze data.

7.2 Deepen justification of the need of the eye gaze as the unique authentication method

Although users mentioned the security concern, that stopped them from adopting the behavioral tracking. However, behavioral tracking is also welcomed, with users aware of it, being a novel way, which has the advantages that the previous password way does not have. Also, if the password-based or existing way of authenticating users is effective, there would be less of the password, the inf oration stealing news appearing. That is why novel authentication methods still exist, despite their safety concern, especially when the security it brings can overcome its inconvenience. E.g., some users mentioned using it for the crypto wallet or banking, where a higher level of security is needed. The study learned on shopping sites is more of a leisure and non-essential situation. However, a system where the concern about authentication or losing one's data (instead of the personal behavioral data) can be done to measure their willingness to lose the data.

7.3 Consistency with the previous works

The results found in Section 6.4 is consistent with a previous study done by [Ste16], which found that only one-fifth of the participants chose to click the link to read the policy, and when users have clicked the link to read the policy, they tend to skim through the text (in comparison with those who have presented the condition by default). In our case, we test to see the condition when part of the condition is shown to the user. When the participants are given 2 of the service and privacy terms to read, if they have read the first one, they tend to skim it and skip the second one, which is consistent with [Ste16]'s study result and add a new perspective.

As a result, 25% of the users reported that the interface or design of the website, whether it looks professional or not, affects their perception of if the website is safe. This is consistent with the finding from [FML+01] on the credibility of a website, where it found that the "look and feel" of a website is the most critical factor in gaining users' trust. Where [DT05] found that the images presented on the web page, which does not confirm or validate the actual security level of online interaction, are considered to be equally as trustworthy by the user. The study by [DTH06] found that 23% of the participants do not look at any of the web browser security indicators; it concluded passive security indicators.

In Section 6.3, the top influence on shopping behaviors, 41.56%, is reported on the products, and 33.33% reported on the price. 16.67% consider the trustworthiness of the companies, the reviews, and the user experience. the result is consistent with Section 2.1 on the shopping online behavior literature. [JPH12] find that most consumers purchase products from the less expensive site when compared between 2 different websites, even when it requires more comprehensive data disclosure. It concluded that even a website's trustworthiness is a concern, but Overall, multiple factors are considered, showing that online shopping is an event that is composed of many considerations.

7.4 Unexpected Results

7.4.1 Different interaction mechanisms affect eye gaze and mouse behavior

With the heat map that visualizes and combines eye gaze tracking with mouse tracking data and the counter-on-increment on the participant's eye gaze and mouse gaze, the result is unexpected in terms of the nature of the eye gaze and mouse. The eye gaze is the genuine feedback captured by the camera, while the result of the mouse position is limited more due to the screen resolution, the record left from the previous page. For example, when a new page is directed from the previous page, the starting position of a mouse would stay at the last position of the previous page. Therefore, the result captured by the mouse may not always show the behavior of a user fully. When a new page is opened, the eye gaze reflects more synchronize to the first reaction of how a user perceives the page, although also limited to some device restriction (e.g., what contents are being shown on the screen at the moment). But the starting point of a gaze match more of the current mental state of the user.

Another observation is that the movement of the mouse has a more limited range than the eye gaze. This could be because the mouse's location is limited to how much space the mouse can move around at the table. It is designed in a way, with the scrolling input, users can perform the task efficiently without moving the hands a lot, which causes move movement created on the heat map more on according to the target location at mind, where eye gaze appear of more of the mental process, e.g., the stage of how the users capture the information is also sown. In other words, the users may perform the mouse movement in the slightest possible motion, and the resulting movement already processed in the user's mind is shown. Moreover, the movement of

the mouse, e.g., at the product page, where the going back and forth repeatedly, by using the go to previous page button have to be a click, the tendency (/ the path) left by the mouse data left indicate not just the behavior according to the user, but also how the system designed to have the mouse interact with the browser. Because when during the measurement of the study interface, the eye gaze, in this case, does not have explicit or implicit interaction with the interface, the collected movements reflect more of the direct output from the user's reaction. In other words, mouse data are recorded significantly on the areas that require mouse interaction. As the nature of a mouse is as an input device. While eye gaze is the natural output from the human.

When designing a system that applies the eye gaze and mouse tracking, the design should consider how much the system and mechanism of the mouse affect the mouse data and not fully reflect the behavioral data. We can see, e.g., in Figure 8.1, the mouse tends not to move horizontally, but in this case, the user has adapted the scrolling on the mouse, where the eye gaze data is left on seeing the picture. However, it is also noticed that the mouse partly synchronizes with the mouse, especially when the users are reading the texts.

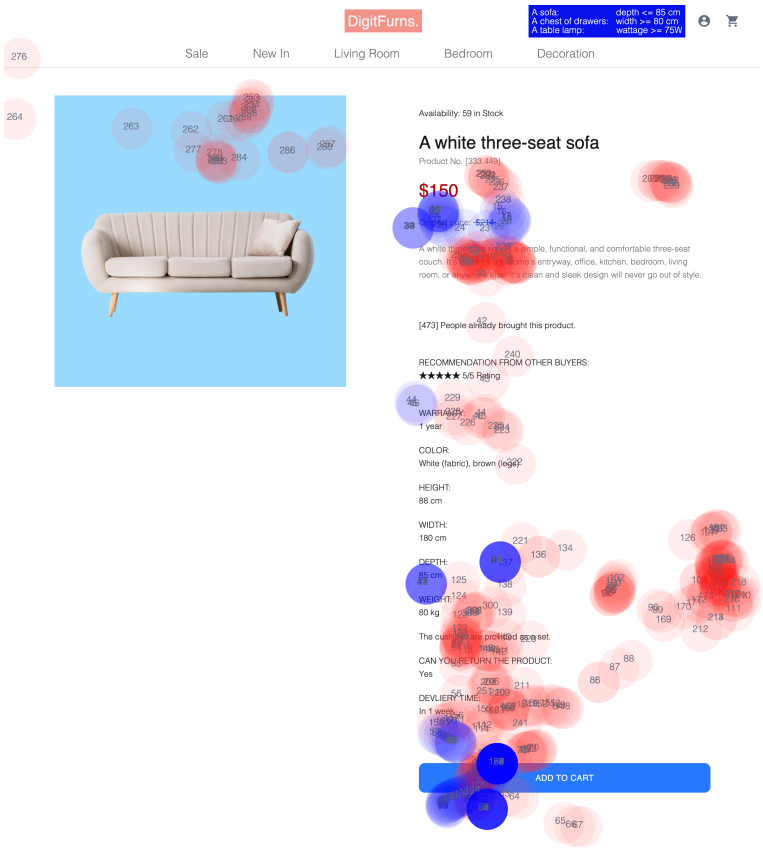


Figure 7.1: Heat map of participant 7 (gaze and mouse position is presented at the same time)

7.4.2 Task difficulty and total attention spent

A clear relationship indicated from the study is the perceived difficulty of the task and the time required to finish the task. We noticed from Section 6.4.1 that the Decoration page's time is significantly higher than other pages. It is reasonable that every product browsing requires opening the products page, and there are many input fields in the register page, making them the first two pages that require time and attention. The tasks that required to perform at the decoration page (to find one product out of the 38 items, with 15.79% of chances of choosing the possible

option), which is similar to what behavior would be performed at the Living Room page and the Bedroom page, but despite no input from the keyboard is needed, this page is recorded with high data records. In Section 6.1 (Demographics), we can see that 25% of participants find that, specifically, finding a lamp with high wattage is challenging, regardless of whether they think the overall task is easy or difficult.

This could be due to the information bundled with the information of the wattage on the table lamp items, where the length of the cord is also provided, with little spacing in between. Compared to information on the product page for items in the living room and bedroom, every information is separated with a gap that helps users distinguish the information they were seeking. Hence, we could sum up that if the information provided is hard to see, users perceive it as difficult, and the result of their opinions on task difficulty is in a positive relationship with the attention recorded on the task. This result shows the positive relationship between the cognitive perception of the task and mouse-tracking data.

7.5 Design a better behavioral tracking system applying the result

Consider the result from Section 6.3 on understanding users' opinions on eye gaze tracking to enhance the account's safety. Three responses represent three types of user groups for a security system. A system that can consider different users' needs can be developed. Also, it is interesting that half of the participants are unwilling to give the eye gaze tracking data. Moreover, half are neutral and positive about it, while the concern for neutral response is the calibration process being slow, and they consider it if the technology is advanced in the future. This lead to the conclusion that half of the people are

7.6 Categorize the use case of behavioral tracking

The usage of eye gaze and mouse tracking can be applied in different cases. Our study was used as the indicator on what users pay attention to, if they have noticed the security cues, and how they interact with the website to understand their behavior in online shopping. However, categorization can be further developed.

Section 6 is mainly concerned with the security of the leaving of eye gaze tracking. We think that better education and defining how different situations can use behavioral data differently and help users make better decisions on if they would be willing to use the system, instead of considering eye gaze data as one big thing. As there is a different type of eye gaze data, the level of detail of how it is collected and the data storage and filtering also affect the detail level of those data. The categorize of the use of behavioral tracking is needed.

7.6.1 For the authentication purpose

Although we did not test if the authentication system works by having the two sessions at the end, we have noticed the power of the information that can be discovered, even with a short period of eye gaze tracking data. The user's feedback could be an attenuating mechanism under certain situations, such as accessing cryptocurrency wallets or banking.

Although there are many reasons why the users may not want to use the system, they consider it an inconvenience while using eye-gaze tracking. However, when eye gaze calibration is not needed, actually implementing eye gaze tracking at a system could save time. It applies to the case when the users have a high frequency of interaction with the system, which already much data is handed to that system, e.g., a system that has the scheduling, many drive data, in the cloud,

that help organize the user's life. Such as Google drive or companies nowadays trying to ask users to adapt to implementing the ire system, put it into life, or accompany in their daily life with the company.

The authentication via SIMS or password can be problematic in some cases. If you are required to log into a system several times per day, checking SMSs and using the phone constantly is a cognitive burden that is troublesome for users. If logging into the system is needed first (e.g., a stock trading system, when you are alerted and want to enter the system, however, rather than waiting for an SMS to arrive, you can log in right away).

In this situation, a high level of authentication is necessary, but the urgency and speed to enter the system in the first place are also needed. Therefore, the authentication can be done by eye gaze and mouse tracking, which provide quick login time, and authenticate later if the user turns out to be a different person after login. As a result, a solution can provide a quick login time while decreasing the cognitive load when users are under pressure (e.g., when entering the stock trading system, with the task's urgency in mind). Users can be considered the identity owner, rather than wasting cognitive load to prevent other users from accessing the system.

7.6.2 For the security alert

As an explicit way of communicating, displaying alerts to the users, then using the eye gaze as the implicit input, the system only alerts when the user has missed the cue on an important area, for the purpose to protect the users' right (e.g., the looking at the security lock the URL while performing the online transaction), look at the terms with enough attention time. This mechanism can be implemented either from the web site's owner (the business), on the client-side, or implemented by the web browser provider as a plug-in already being able to be provided to the browser user. According to the chapter on the theoretical background, studied by [RLR00] [WGF+87] found that the warning system is more effective when the severity of the consequence is given. Thus, the alert can combine the potential consequence, e.g., what happens when not looking at the secured transmissions layer of an online connection and the privacy terms.

7.6.3 Communication between more than one users

With interaction with the online shopping site, the user may not be willing to provide the data in exchange. However, when considering a system to provide communication with friends or colleagues, where the users do not want to share their appearance online, or they cannot share high-quality video or audio online, due to technical limitation, the eye gaze authentication can be used at this case, because the data processing from video input to eye gaze data point can be processed at the client's side. Only the information of the gaze point or the validation statement can be sent to the server. The opinions of if the users feel more safe knowing that the friend they communicated online is the actual person they intended to talk with would provide an incentive for them to adapt the eye gaze tracking.

7.7 Different level of applying behavioral tracking permitted by the users

Not all the pages or functions require eye gaze tracking. Furthermore, Eye tracking and mouse tracking may not need to be the only way of authentication. The user mentioned that they would prefer their authorization and opt for password-based attenuation as the first option. The user's consent and want to be informed of what data and be active in adopting such a service is known from Section 6 (Result). A more flexible solution considering different users' perspectives and needs can be offered to enhance the adaption of the method.

Level of applying of behavioral tracking	The main concern of the system	The sacrifice for concern
Low	Reminder of security cue	Absence of authentication (no data storage)
Middle	Convenience and user experience	Primary authentication by traditional method
High	System security and protection	The user cannot opt out of eye gaze tracking

Table 7.1: Level of adaption of behavioral tracking and principles

7.7.1 Low level – a detection of the eye gaze attention

Considering that eye gaze tracking has many applications, not every eye gaze tracking needs to leave a record in the system's database. The system does not require behavioral data to act as a tool to assist the user in achieving a higher level of security by detecting their eye gaze attention and making a reminder. The use of eye gaze as a reminder of attention and authentication is possible at the same time in this system.

7.7.2 Middle level – an extra level of security

Eye gaze tracking can be implemented in the system, but it does not always have to be the primary authentication method. Such a system would use eye-gaze tracking for convenience, with the user experience as its core.

7.7.3 High level – a must of tracking and storage of behavioral

System security is important when handling sensitive information; therefore, a high level of security is needed. In addition, behavioral data needs to be collected in order to improve the accuracy of the data. In this case, authentication should be prioritized over user convenience. This method can benefit both the users and the company if everyone agrees to it.

8 Conclusion

The study investigates the user's behavior by using eye gaze tracking and mouse tracking. There are expected results that match the literature research, such as the level of user awareness of the security cue on a website is low. In the absence of correct interventions, advice for users, or public education, this situation appears unlikely to change with the online payment system interface remaining the same.

Using the tools of eye gaze tracking, mouse tracking, heat maps generated by these data, and statistical analysis, we showed some insights into the user's mental process during the online shopping and payment process. The study also found the fundamental difference of the traditional way of authentication (e.g., password and SMS), using mouse tracking and eye gaze tracking, respectively.

With the understanding of the different applications of security measures on a website, the survey results take the user's perspective. This study found a discrepancy between users' knowledge of eye gaze tracking and its possible usage. Moreover, the study provided a schema to suggest how to include the behavioral tracking into a system by understanding the concern and the willingness of sacrifice in exchange for the concern. The suggestion is that behavioral tracking can be used as a reminder or a primary way to authenticate a user.

The study also concludes with a discussion of how eye gaze tracking can be used in the current situation when society has started interacting mostly online rather than in person. The number of online shoppers is expected to increase, as well as the number of online communications. The behavioral tracking relies only on retrieving the data, which can benefit from requiring less bandwidth, and users' faces are not being stored. It can be used as an extra authentication method to facilitate certificated communication.

In addition, the study provided an insight into how eye gaze tracking with user data can be used. In the future, researchers can continue on this investigation and deepen the understanding of the specific area.

9 Future Work

9.1 Study for situation required a higher level of security

Although at the study, the payment and password registration situation were appeared and measured, as it is a critical security situation. However, the shopping site information contents are not at a deep concern in terms of the importance of the data. It is possible to test the situation requiring higher security, such as banking or a crypto wallet, to determine if the user considers behavioral data an extra security level.

9.2 Study on authentication for communication

In this study, we measure the security measurement on the shopping website. However, a situation where two users can authenticate themselves without showing their face online can be achieved with behavioral tracking. This method is helpful when the need for online and distant learning or work is high. For example, during an online exam, eye gaze tracking can be the alternative for authentication when the authentication on the face is not possible (due to limitation of the video bandwidth or technical difficulty), and participant's numbers can be up to a hundred. Behavioral tracking can require the lower transmission of data because the data is calculated and transformed at the client-side first before sending it to the server for analysis.

9.3 Study on promoting awareness of using behavioral authentication

Users are concerned about eye gaze because they equate it with collecting a comprehensive set of biometric data. However, behavioral authentication can be safer in some cases because it is hardly learned by others quickly. Not knowing the mechanism and the different levels of ability to use the technology hinder the adoption of this technology. Companies like Microsoft have studies on preparing the age of need for behavioral data to design a system to protect users' rights. Studies on what factors affect the detection of the users on behavioral authentication can be investigated to promote the use of this technology.

10 Appendix

10.1 Survey Questions

- Q1: Please select your sex:
  Male, Female, Other, Prefer not to say
- Q2: What is your age?
- Q3: Which country do you live in?
- Q4: What is your profession?
- Q5: Which online shopping platform do you use the most when shopping online? (e.g., Amazon, Zalando, Otto, H&M, IKEA, eBay, etc.)?
- Q6: Which device(s) did you use the most often when shopping online?
  Desktop, Laptop, Smartphone, Tablet, Others
- Q7: Which payment method(s) did you use the most when shopping online?
  Credit card, PayPal, Bank transfers, Debit Card, GiroPay, Invoice, SEPA-Lastschrift (Direct Debit), Cash-on-delivery, Sofort, Other
- Q8: How often do you shop online?
  None, Less than once per quarter year (3 months), Once per quarter year (3 months), 2 times per quarter year (3 months), Once per month, 2 to 3 times per month, Once per week, 2 to 3 times per week, Once per day

Please indicate how much you agree or disagree with the following statements. (Strongly Disagree to Strongly Agree)

- Q9: I have experience with IT Security.
- Q10: I am proficient at using the computer.
- Q11: I have experience with using eye tracking.
- Q12: My eyes felt tired after or during the study.
- Q13: At the registration page of the experiment, I used the password suggestion to help my password creation process.
- Q14: At the payment stage of the experiment, the privacy term reduced my concern about online transaction safety.
- Q15: I am more willing to shop on a website knowing my account is safely protected.
- Q16: I am more willing to shop on a website knowing my account is safely protected through eye gaze tracking authentication (i.e. the system will alert when it has detected another user is trying to pretend to be me)

- Q17: I am willing to leave my eye gaze behavioural data (i.e. the record of my eye gaze behaviour while shopping at a website) knowing the company is authorized by me to process my personal information (e.g. the credit card information and the username) already.
- Q18: I will shop more often on the same website, knowing that the more I shop, the more accurate the authentication system (to protect my account) will be.

(Keywords are enough for answering the following questions.)

- Q20: What usually affects your shopping behaviour online (i.e. where to shop and what to buy)?
- Q21: What aspect(s) makes you feel the online transaction is safe on an online store?
- Q22: Would you like to have eye gaze tracking being used to enhance your account's safety (i.e. the system will alert when it has detected another user trying to pretend to be you)? Why (and why not)?
- Q23: Do you find the tasks given in the experiment difficult? Why (and why not)?
- Q24: What are your other opinions about the eye gaze, mouse tracking and the experience of the experiment (that is not mentioned above)?

10.2 Repository content

The following files are provided at the submission folder.
1. ReactJS project repository
2. Statistic and analysis of the collected data
3. Generated graphic from Statistic and analysis of the collected data
4. Heap Maps
5. Programme to generate heat map
6. Data snippets from the participants
7. Survey responses
8. Thesis Latex file

References

[AVK+16] ANDERSON, Bonnie B. ; VANCE, Anthony ; KIRWAN, C B. ; JENKINS, Jeffrey L. ; EARGLE, David: From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. In: *Journal of Management Information Systems* 33 (2016), Nr. 3, S. 713–743

[BJM09] BARTH, Adam ; JACKSON, Collin ; MITCHELL, John C.: Securing frame communication in browsers. In: *Communications of the ACM* 52 (2009), Nr. 6, S. 83–91

[BVOP+09] BIDDLE, Robert ; VAN OORSCHOT, Paul C. ; PATRICK, Andrew S. ; SOBEY, Jennifer ; WHALEN, Tara: Browser interfaces and extended validation SSL certificates: an empirical study. In: *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, S. 19–30

[Can21] CANVA: *Canva's Content License Agreement.* https://www.canva.com/policies/content-license-agreement/. Version: 2021

[DT05] DHAMIJA, Rachna ; TYGAR, J D.: The battle against phishing: Dynamic security skins. In: *Proceedings of the 2005 symposium on Usable privacy and security*, 2005, S. 77–88

[DTH] DHAMIJA, R ; TYGAR, JD ; HEARST, M: Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems. In: *CHI* Bd. 6, S. 581

[DTH06] DHAMIJA, Rachna ; TYGAR, J D. ; HEARST, Marti: Why phishing works. In: *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, S. 581–590

[Duc02] DUCHOWSKI, Andrew T.: A breadth-first survey of eye-tracking applications. In: *Behavior Research Methods, Instruments, & Computers* 34 (2002), Nr. 4, S. 455–470

[FB95] FURNESS, THOMAS A. ; BARFIELD, WOODROW: Advanced Interface Design. In: *Virtual Environments and Advanced Interface Design* (1995), S. 1

[FML+01] FOGG, Brian J. ; MARSHALL, Jonathan ; LARAKI, Othman ; OSIPOVICH, Alex ; VARMA, Chris ; FANG, Nicholas ; PAUL, Jyoti ; RANGNEKAR, Akshay ; SHON, John ; SWANI, Preeti u. a.: What makes web sites credible? A report on a large quantitative study. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2001, S. 61–68

[Fou22] FOUNDATION, OpenJS: *Introduction to Node.js.* https://nodejs.dev/learn. Version: 2022

[Ger] GERMANY, Ikea: *Ikea Germany.* https://www.ikea.com/de/de/

[goo22] *Secure your site with HTTPS.* https://developers.google.com/search/docs/advanced/security/https. Version: 2022

[Hao12] HAOYU, Wang: Privacy, How Can I Protect You? How to Construct Safe Data Security System in E-commerce Transaction. In: *2012 Fourth International Conference on Computational and Information Sciences* IEEE, 2012, S. 441–444

[HM] HM: *HM Germany.* https://www2.hm.com/de_de/index.html

[HNN+18] HESSELS, Roy S. ; NIEHORSTER, Diederick C. ; NYSTRÖM, Marcus ; ANDERSSON, Richard ; HOOGE, Ignace T.: Is the eye-movement field confused about fixations and saccades? A survey among 124 researchers. In: *Royal Society open science* 5 (2018), Nr. 8, S. 180502

[Hom] HOME, Zara: *Zara Home.* https://www.zarahome.com/de/en/

[JPH12] JENTZSCH, Nicola ; PREIBUSCH, Sören ; HARASSER, Andreas: Study on monetising privacy: An economic model for pricing personal information. In: *ENISA, Feb* 1 (2012), Nr. 1

[KAR+20] KATSINI, Christina ; ABDRABOU, Yasmeen ; RAPTIS, George E. ; KHAMIS, Mohamed ; ALT, Florian: The role of eye gaze in security and privacy applications: Survey and future HCI research directions. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, S. 1–21

[LAS13] LECLAIR, Jane ; ABRAHAM, Sherly ; SHIH, Lifang: An interdisciplinary approach to educating an effective cyber security workforce. In: *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, 2013, S. 71–78

[LL00] LIANG, Ting-Peng ; LAI, Hung-Jeng: Electronic store design and consumer choice: an empirical study. In: *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* IEEE, 2000, S. 10–pp

[Mad] MADE: *About MADE.* https://www.made.com/about-us

[MB14] MAJARANTA, Päivi ; BULLING, Andreas: Eye tracking and eye-based human–computer interaction. In: *Advances in physiological computing*. Springer, 2014, S. 39–65

[MP22] META PLATFORMS, Inc.: *React. A JavaScript library for building user interfaces*. https://reactjs.org/. Version: 2022

[MyC] MYCONCEPT: *MyConcept.* https://www.myconcept.com.hk/

[Pex] PEXELS: *Free Stock Photo. Video License - Pexels*. https://www.pexels.com/license

[PUM19] PFEFFEL, Kevin ; ULSAMER, Philipp ; MÜLLER, Nicholas H.: Where the user does look when reading phishing mails–an eye-tracking study. In: *International Conference on Human-Computer Interaction* Springer, 2019, S. 277–287

[Ray98] RAYNER, Keith: Eye movements in reading and information processing: 20 years of research. In: *Psychological bulletin* 124 (1998), Nr. 3, S. 372

[RLR00] ROGERS, Wendy A. ; LAMSON, Nina ; ROUSSEAU, Gabriel K.: Warning research: An integrative perspective. In: *Human Factors* 42 (2000), Nr. 1, S. 102–139

[SBVOP08] SOBEY, Jennifer ; BIDDLE, Robert ; VAN OORSCHOT, Paul C. ; PATRICK, Andrew S.: Exploring user reactions to new browser cues for extended validation certificates. In: *European Symposium on Research in Computer Security* Springer, 2008, S. 411–427

[Sc17] STRONGLOOP, IBM ; CONTRIBUTORS other e.: *Express. Fast, unopinionated, minimalist web framework for Node.js.* https://expressjs.com/. Version: 2017

[SDOF07] SCHECHTER, Stuart E. ; DHAMIJA, Rachna ; OZMENT, Andy ; FISCHER, Ian: The emperor's new security indicators. In: *2007 IEEE Symposium on Security and Privacy (SP'07)* IEEE, 2007, S. 51–65

[SEA+09] SUNSHINE, Joshua ; EGELMAN, Serge ; ALMUHIMEDI, Hazim ; ATRI, Neha ; CRANOR, Lorrie F.: Crying wolf: An empirical study of ssl warning effectiveness. In: *USENIX security symposium* Montreal, Canada, 2009, S. 399–416

[Ste16] STEINFELD, Nili: âI agree to the terms and conditionsâ:(How) do users read privacy policies online? An eye-tracking experiment. In: *Computers in human behavior* 55 (2016), S. 992–1000

[WGF+87] WOGALTER, Michael S. ; GODFREY, Sandra S. ; FONTENELLE, Gail A. ; DESAULNIERS, David R. ; ROTHSTEIN, Pamela R. ; LAUGHERY, Kenneth R.: Effectiveness of warnings. In: *Human Factors* 29 (1987), Nr. 5, S. 599–612

[WI05] WHALEN, Tara ; INKPEN, Kori M.: Gathering evidence: use of visual security cues in web browsers. In: *Proceedings of Graphics Interface 2005* Citeseer, 2005, S. 137–144

[Wog18] WOGALTER, Michael S.: Communication-human information processing (C-HIP) model. In: *Forensic Human Factors and Ergonomics*. CRC Press, 2018, S. 33–49