Yousra Javed* and Mohamed Shehab

Look Before You Authorize: Using Eye-Tracking To Enforce User Attention Towards Application Permissions

Abstract:
Habituation is a key factor behind the lack of attention towards permission authorization dialogs during third party application installation. Various solutions have been proposed to combat the problem of achieving attention switch towards permissions. However, users continue to ignore these dialogs, and authorize dangerous permissions, which leads to security and privacy breaches.

We leverage eye-tracking to approach this problem, and propose a mechanism for enforcing user attention towards application permissions before users are able to authorize them. We deactivate the dialog's decision buttons initially, and use feedback from the eye-tracker to ensure that the user has looked at the permissions. After determining user attention, the buttons are activated. We implemented a prototype of our approach as a Chrome browser extension, and conducted a user study on Facebook's application authorization dialogs. Using participants' permission identification, eye-gaze fixations, and authorization decisions, we evaluate participants' attention towards permissions. The participants who used our approach on authorization dialogs were able to identify the permissions better, compared to the rest of the participants, even after the habituation period. Their average number of eye-gaze fixations on the permission text was significantly higher than the other group participants. However, examining the rate in which participants denied a dangerous and unnecessary permission, the hypothesized increase from the control group to the treatment group was not statistically significant.

Keywords: Habituation, Human Factors, Privacy, Permissions Dialogs, Third Party Applications, Eye-Tracking

DOI 10.1515/popets-2017-0014
Received 2016-08-31; revised 2016-11-30; accepted 2016-12-01.

***Corresponding Author: Yousra Javed:** University of North Carolina Charlotte, E-mail: yjaved@uncc.edu
Mohamed Shehab: University of North Carolina Charlotte, E-mail: mshehab@uncc.edu

1 Introduction

Third party applications are being widely used today. The two main avenues include mobile phones and social networks. Third party application developers require user permissions to acquire read or write access to user data in accordance with the application's functionality. These permissions are presented to the user (through the scope parameter) on the installation dialog as part of the authorization flow. The user is supposed to review the permissions before going ahead with the installation or canceling it. Once the permissions are granted and the authorization flow is completed, the application receives an access token, which the third party developer uses to make API calls on behalf of the user to retrieve user data [3].

The phenomenal growth of the Facebook and Android platform in the past few years has made them a lucrative target of malicious application developers and spammers. Installing malicious applications or authorizing unnecessary permissions without reading and consenting to them raises the risk of unintentional information disclosure to third parties. A Wall Street Journal study found numerous apps on Facebook extracting identifiable user information from the platform and sharing this bounty with advertising companies [20]. *Facebook color changer* is a malicious application that steals the user's Facebook access tokens [5]. Similarly, lookalike applications of popular Facebook applications such as *Candy Crush Saga* have been used to target users. Rehman et al. [18] state that malicious apps request more permissions than benign apps. In 2015, the *Most Used Words* quiz application on Facebook was accused of stealing user data since the application was requesting many more permissions than required for its functionality [4]. Chia et al. [11] showed that free, and lookalike applications request more permissions than is typical. For example, the flashlight android application

asks for wifi and location permissions which are not required for its functionality [1].

Many users do not pay attention to the permissions requested by third party applications. Habituation is one of the main factors behind the lack of user attention towards the application installation dialogs. When non-compliant behavior does not cause harm over time, people may develop an automated response, habituation, that does not take into account changes in warning context or messaging [16]. Habituation decreases warning effectiveness when people become less alert to the information presented in warnings. Felt et al. [13] found that only 17% of phone users paid attention to permissions during application installation. Since security is not the primary task of the user, repetitive appearance of the same warning/dialog with no serious consequences trains the user to react to it in a certain way without reading or paying attention to it. Many attractors [9] and polymorphic warning designs [6] have been proposed to combat similar problem in warnings. Similarly, several risks signals have been proposed to inform the user about the risks associated with the application installation by using various features such as permissions the application requests, its category, what permissions are requested by other applications in the same category, and the user's personal information examples [15, 19]. However, to the best of our knowledge, the use of eye-tracking has not been explored to enforce user attention.

Looking at the permissions is the first step in assessing the risks involved with application installation. We propose an eye-tracking based mechanism of enforcing user attention on application permissions. Our approach is inspired by two existing systems. First is a mechanism on various websites to ensure that the user has read the privacy/ consumer policies before clicking on the *I Agree* button. The decision buttons are initially deactivated, and once the user reads and scrolls down on the policy, they are activated. Second is an eye-tracking based mechanism to put the user into the habit of looking at the URL address bar to determine the website's legitimacy before entering sensitive information[17]. The input fields are initially deactivated, and once the user looks at the URL address (determined using the eye-gaze fixations on the URL address bar screen coordinates), they are activated. We deactivate the decision buttons on the dialog, and use feedback from the eye-tracker to ensure that the user has looked at the permissions. After determining user attention, the decision buttons on the dialog are activated. We implemented a Chrome browser extension for this purpose. The extension deactivates the decision buttons when it detects an application authorization dialog. It then uses a web-socket to receive eye-gaze data from the eye-tracking module. Based on the overlap of the received eye-gaze coordinates and the permission coordinates on the screen, the extension determines when to enable the decision buttons on the dialog.

We conduct two experiments to test the effectiveness of our approach. The first experiment tests whether the user pays more attention to the permissions when using our system. The second experiment studies our system's resistance against habituation. Due to the difficulty of testing eye-tracking on mobile applications, we focus on authorization dialogs for desktop web applications. We chose Facebook applications for this purpose.

In this paper, we contribute the following:

- We propose an eye-tracking based mechanism of enforcing user attention on the application permissions.
- We implement a prototype of our proposed system and conduct two experiments to evaluate its effectiveness.
- We show our approach's preliminary evaluation through two experiments. Our first experiment on 60 participants tested the participants' attention, where as, our second experiment on 45 participants focused on our approach's resistance to habituation. Using participants' eye-gaze fixations, permission identification, and authorization decision, we evaluate our participants' attention towards permissions.

2 Related Work

The literature most relevant to our work falls in three main categories: attention attractors and warning designs; application risk signal communication; and eye-tracking applications in user attention and comprehension.

2.1 Attention attractors and warning designs

Bravo-Lillo et al. [9, 10] proposed five attractors to draw users' attention to a text field within a dialog. Among these, four were inhibitive attractors which prevent the user from proceeding until some time has passed (such as waiting for the text to gradually appear or become highlighted) or, the user performs a

required action (such as moving mouse over a field or typing the text). One attractor was non-inhibitive and included an attention-grabbing stylistic change of text font and background. They studied the attractors' resiliency to habituation. The two inhibitive attractors that forced the user to interact with the text field by moving mouse over it or typing the text proved to be effective even after increasing the level of habituation.

Anderson et al. [6] proposed a polymorphic warning design that changes its appearance. They use functional magnetic resonance imaging (fMRI) and mouse cursor tracking in their experiments to show that their polymorphic warning is effective in combating habituation as compared to the conventional warnings.

2.2 Application risk signal communication

Several researchers have made efforts to improve the risk communication on authorization dialogs. Egelman et al. [12] proposed design changes to the Facebook connect dialog by presenting the actual information requested by the public profile permission. They observed that the changes were noticed, but because users had such low expectations for privacy, that the additional information did not dissuade them.

Harbach et al. [15] proposed a modified permission dialog for android applications to improve security risk communication to the end-user. They present personal information example along with each permission to help the user understand the risk associated with a permission's authorization. Their study showed a significant difference in the behaviors of participants who were presented with modified dialog design as compared to the ones presented with the default design. The participants who were shown information examples for each permission spent more time on the dialog and appeared to be more aware of the security and privacy risks. However, they used sample data for their study and did not explore the use of actual user information.

Sarma et al. [19] proposed a mechanism of creating effective risk signal for android applications that 1) is easy to understand by both the users and the developers; 2) is triggered by a small percentage of applications; and 3) is triggered by many malicious applications. They use both the permissions an application requests, the category of the application, and what permissions are requested by other applications in the same category to better inform users whether the risks of installing an application is commensurate with its expected benefit.

Social navigation is defined as the use of social information to aid a user's decision. Besmer et al. [8] have explored the use of social navigation cues (e.g., the percentage of users who have allowed/denied a particular permission) in helping the users make better permission authorization decisions when installing Facebook applications. They find that social cues have barely any effect on users' Facebook privacy settings. Hence, only the small subset of users who take the time to customize their settings may be influenced by strong negative social cues.

2.3 Eye-tracking for user attention and comprehension

Eye-tracking has been passively used to analyze user attention and comprehension by observing the frequency and duration of user's eye-gaze over security indicators and permission dialogs. Furman et al. [14] conducted an eye-tracking experiment on the Facebook connect dialog formats proposed by Egelman et al. [12] i.e., with and without information verbatim. Their results showed that although the participants who were shown information verbatim took longer to read the dialog, it did not affect their decision to authenticate using Facebook connect. Arianezhad et al. [7] used eye-tracking to study whether computer or security expertise affects the use of web browser security indicators. Their eye-tracking data showed that the users with security expertise have longer eye-gaze duration at security indicators than those without security expertise. Whalen et al. [21] used eye-tracker to study user's attention to browser security. They found out that without being primed to security, no participants viewed security indicators.

The eye-trackers are gradually becoming cheap and affordable, and will soon be embedded inside smartphones and computers. Therefore, researchers are now experimenting with active applications of eye-tracking. Miyamoto et al. [17] have developed EyeBit—an eye-tracking based system to inculcate the habit of looking at the URL address bar before entering sensitive information in the website's input fields, in order to prevent phishing. The system first deactivates the input fields in a website, and using the eye-tracking data determines if the user has looked at the website's URL. The input fields are activated after confirming user attention on the URL address bar. Their system showed good learnability, and improved the accuracy of detecting phishing websites.

3 Eye-Activated Permission Authorization

This section introduces a mechanism to enforce end-user attention towards the application's requested permissions at install-time. Section 3.1 summarizes the overview and our assumption, that is, forcing the end-users to look at the permissions will be beneficial for them. Section 3.2 presents the design and implementation of our proposed scheme.

3.1 Overview

In this paper, we speculate that forcing the user to look at the permissions is the first step towards combating habituation and installing safe applications. Once, the user gets into the habit of looking at the permissions, this action will often be performed unconsciously. Even if the primary concern of the end-user is not security, the habit would work like a conditioned reflex action. The habit will also improve the chance of being aware of the security information.

In our pilot study, we analyzed the eye-gaze data of 16 participants on permission authorization dialog as they installed Facebook applications. Figure 1 shows a heatmap of eye-gaze fixations on various regions of the dialog. The red region shows the areas users looked for a longer duration, while the green region shows the areas where the users looked for a shorter duration. It can be observed from the figure that the majority of participants did not spend enough time on the dialog text to demonstrate that they had read the text.

We propose and develop a mechanism for enforcing user attention towards application permissions. Using eye-gaze data, we determine if the users look at a particular portion of the dialog on the screen. Failing to look at the permissions text area prevents the users from continuing the installation process.

3.2 Design and Implementation

Our system has the following features.

- Dialog button control
  Our system has functions to detect and activate/deactivate the buttons on installation dialog. The system deactivates the "Allow" and "Deny" buttons on the dialog, at first. When it detects that the user has checked the permissions displayed on the dialog, these buttons are then activated.
- Eye-tracking
  Our system interacts with the eye-tracking device, and identifies that the user has looked at a particular portion in the web browser with certainty.
- Permission localization
  Our system is able to locate the application's permission text within the screen (assuming a maximized browser for the time being).

Fig. 1. Heatmap of eye-gaze fixations on Facebook application authorization dialog (as of early 2015)

The architecture of our system is shown in Figure 2. It consists of an eye-tracking module, and a browser extension module. The browser extension module deactivates all decision buttons on the dialog at first. The task of the eye-tracking module is to interact with an eye-tracker and retrieve eye-gaze fixation coordinates. The eye-tracking module communicates with the eye-tracker server over a TCP socket connection, and retrieves the eye-gaze positions using the tracker API. The browser extension module receives these coordinates from the eye-tracking client module through a web socket, and determines whether user looked within the permissions' text area. The buttons are activated when at least 30 consecutive eye-gaze fixations (measured at 10 eye-gaze fixations per second) are found in that area. This is equivalent to spending approximately 3 seconds scanning permission text area. We used The Eye-Tribe eye-tracker [2] as the eye-tracking device. Its software development kit (SDK) embeds the function of web server

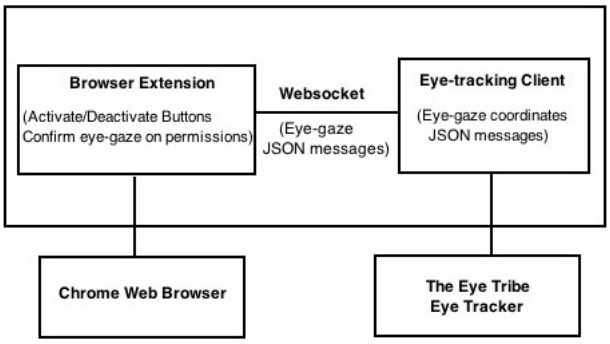


Fig. 2. System Architecture

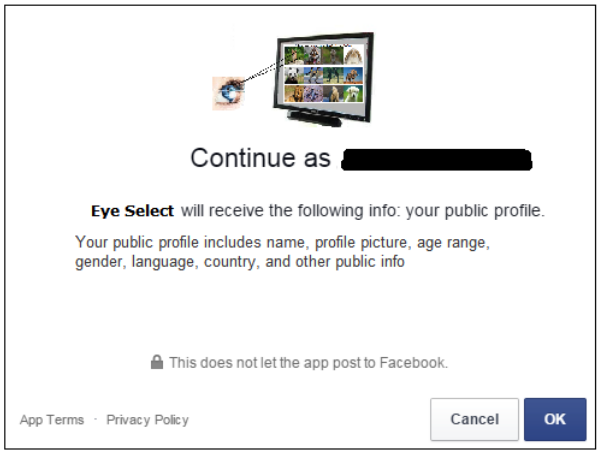


Fig. 3. Eye-Select Facebook application dialog used in our study

and provides the user's eye-gaze position in JavaScript Object Notation (JSON) format messages.

The limitation of our prototype was the localization of the permissions. We estimated the absolute position of the permission text on the screen, assuming the browser's window is maximized.

4 Evaluation

We used two experiments to evaluate our approach's effectiveness on Facebook's existing application installation dialog (see Figure 3). The experiments were approved by UNC Charlotte's IRB[1]. Our first experiment intends to measure user attention towards the permissions displayed on the dialog. The second experiment focuses on measuring our system's resistance to habituation. We paid each participant a $5 Starbucks gift card at the end of the study.

4.1 Experiment 1: Attention

Our first experiment focused on measuring participant attention towards the permissions. We used a between-subjects design for this experiment. We placed participants either in the control or treatment group; exposure to both might have led the participants to suspect that we were studying the installation dialogs. In order to maintain ecological validity, and more closely study participant behavior, some amount of deception was used. We did not tell the participants that they were participating in a security/privacy related study, and were asked to evaluate the feasibility of an eye-activated browser by performing a set of tasks that involved eye-tracking.

4.1.1 Methodology

We recruited our participants through Craigslist, and word of mouth. We advertised our study on Craigslist and the eligible candidates were invited to campus for participation. We also asked the participants to spread the word about our study without revealing the actual goal of the study.

4.1.1.1 Conditions

We compared participants' attention using our proposed approach to two other mechanisms. Therefore, our experiment had three conditions:

- Control - The participants in this group installed the applications using the default mechanism.
- Control with time constraint - The participants in this group spent 3 seconds (equivalent to 30 eye-gaze fixations) on the dialog before they made their decision. The decision buttons were activated after 3 seconds, instructing the participants to proceed. We added this condition to serve as a better indicator of whether spending more time on a dialog leads to better attention as compared to our proposed system.
- Treatment - The participants in this group performed eye-gaze based button activation while installing an application. They were asked to look at the dialog's permission text area to activate the de-

1 IRB Protocol #13-03-30

cision buttons, and then proceed with the installation.

4.1.1.2 Tasks

The participants first logged into their Facebook account. We then briefed them about the tasks which involved eye-tracking. These tasks were implemented as Facebook applications which the participants installed and used. They also had the option of not installing an application. If the participants chose not to install an application, it did not harm our experiment since we were studying the dialog and not the application's functionality. Therefore, in such scenario, the participants were simply taken to the next application. We used the following three applications in our experiments:

- Eye-select application - This application asked participants to select an image by focusing their eyes on it. The participants selected a specific animal's image (for example, a lion) from the set of displayed animal images by finding and fixating on that animal's image until a popup confirming the selection appeared. The participants could continue to use the application if they wished. This application requested access to public profile information.
- Eye-draw application - This application asked participants to draw something on the screen using eye-gaze. The participants drew an object using their eye-gaze. This application requested access to public profile information.
- Eye-chase application - This is an eye-tracking based game in which the participant followed a set of random circles on the screen with his eye-gaze. The installation dialog for this application requested a Social Security Number (SSN) access permission, in addition to the public profile permission requested by the other two applications. Although SSN is never requested by any application, we chose it because the goal of our study was to see if participants would pay attention and identify strange text on the dialog.

The participants first installed and used the eye-select and eye-draw applications (order randomized), and finally installed and used the eye-chase application, and completed the post survey. All participants completed a nine point eye-calibration process before using the applications.

4.1.1.3 Post Survey

Each participant completed a questionnaire at the end of the experiment. The first set of questions asked the participants about their eye-tracking experience. To determine whether participants had noticed the permissions requested by the applications, they were asked questions related to the permissions. We asked the participants to write down the content displayed in each of the three dialogs. Next, the participants identified which of the displayed permissions were requested by the applications presented to them. In the end, the participants provided demographic information. After the participants completed the questionnaire, we informed them about the goal of our experiment.

4.1.1.4 Dependent Variables

We used the following metrics to measure participant attention on the authorization dialog's permissions:

- Permission identification- The fraction of application permissions identified correctly. The requested permissions were public profile information and social security number.
- Eye-gaze fixation- The number of eye-gaze fixations on the permission text area of an application authorization dialog. An eye-gaze fixation refers to the maintenance of visual gaze at a single location.
- Authorization decision- The fraction of social security number permissions denied.

4.1.2 Participants

We ran our experiment between 1st Sept and 10th Oct 2016. A total of 60 participants completed the experiment–20 per group. Table 1 shows our study participant demographics.

4.1.3 Eye-tracking Device

We used **The Eye Tribe**[2] eye-tracker to retrieve eye-gaze information in our experiments. This eye-tracker can detect movement of the pupil with sub-millimeter precision. The average accuracy is around 0.5 degrees of visual angle. The system is capable of determining the on-screen gaze position roughly within the size of a

2 https://theeyetribe.com

Age	n=60	% of n
18 to 20	9	15%
21 to 30	40	66.6%
31 to 40	11	18.3%
Gender		
Male	29	48.3%
Female	31	51.6%
Ethnicity		
Asian/Pacific Islander	36	60%
White/Caucasian	13	21.6%
Middle East	3	21.6%
Black/African-American	1	1.6%
Hispanic	1	1.6%
Decline to answer	2	3.3%
Education Level		
Bachelor's degree	28	38.3%
Master's degree	18	30%
Other	7	11.6%
Some college	7	11.6%
Associate's degree	5	8.3%

Table 1. Participants demographics for the attention experiment

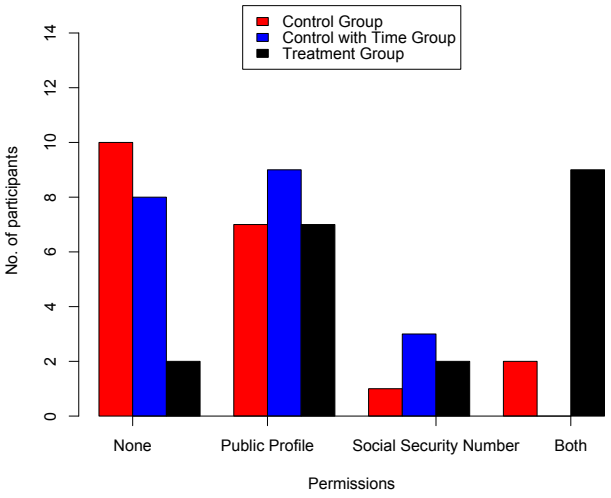


Fig. 4. Number of participants who identified one or both permissions (Attention)

fingertip (<10mm). All precision measurements in our experiments were done at 60Hz sampling rate.

4.1.4 Results

To determine how each dependent variable (attention metric) differed for the independent variable (installation mechanism), we conducted the Kruskal-Wallis test for each dependent variable below. We used Bonferroni correction to account for multiple tests being run. Therefore, we accepted statistical significance at p< .016.

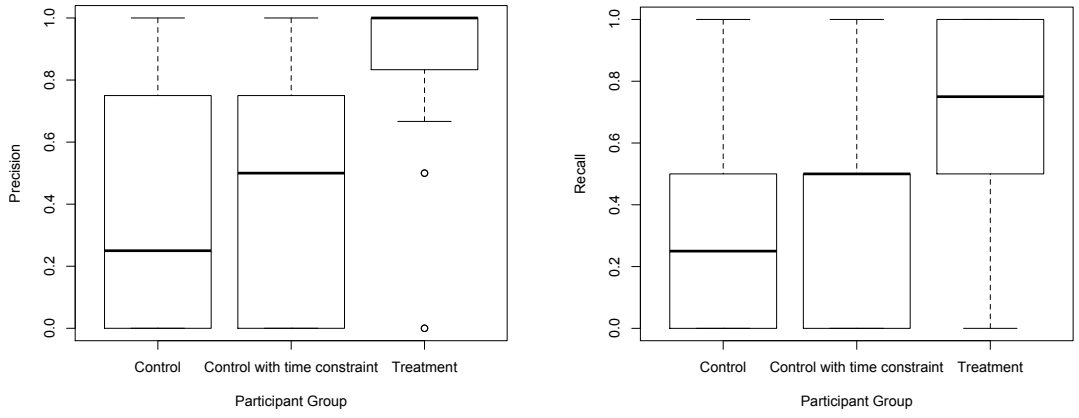
– **Permission Identification**
We first analyzed whether there is a significant difference between the three participant groups with respect to the fraction of permissions identified correctly on the application installation dialogs. The post-survey questions asked the participants to select all the permissions requested by the three applications. We used this response to calculate the fraction of permissions correctly identified by the participants. Figure 4 shows the number of participants in each group who identified the public profile information, social security number, or both permissions. The participants who used eye-activated dialogs were able to identify both permissions better compared to the other two groups.

The Kruskal-Wallis test showed a significant difference between the number of permissions correctly identified by the participants in the treatment group (mean=0.67, SD=0.37), the participants in the control group (mean=0.3, SD=0.34), and participants in the control with time constraint group (mean=0.27, SD=0.34) with p=0.001862.
Post-hoc comparisons using Nemenyi test, showed that there is a significant difference between the number of permissions correctly identified by the control and treatment group with p = 0.015, and between the control with time constraint and treatment group with p=0.0084.
We also calculated the precision and recall for the permissions identified by the participants. We calculate the precision and recall for each participant as follows.

$$\text{Precision} = \frac{\text{No. permissions correctly identified by participant}}{\text{No. permissions selected by participant}} \quad (1)$$

$$\text{Recall} = \frac{\text{No. permissions correctly identified by participant}}{\text{No. permissions requested by the applications}} \quad (2)$$

Figure 5 shows the permission identification precision and recall averaged over all the participants. The average precision and recall was higher for both the control with time constraint group, and treatment group, as compared to the control group.



(a) Precision (b) Recall

Fig. 5. Participant permission identification precision and recall during the attention experiment

– **Eye-Gaze Fixations**
We used eye-gaze fixation count as another metric for measuring participant attention towards application permissions. We logged the participants' eye-gaze coordinates while they were interacting with the installation dialogs. We defined an area of interest around the permission text area and only counted the eye-gaze fixations within this area of interest.
Kruskal-Wallis test showed a significant difference between the number of eye-gaze fixations of the control group (mean= 14.16, SD= 19.12), control with time constraint group (mean=33.3, SD=30.08), and treatment group (mean= 38.2, SD= 6.7) averaged over the three applications' dialogs with p=0.0003. Pairwise comparisons using Nemenyi test showed that the treatment group had significantly more eye-gaze fixations than the control group with p=0.00019. However, the difference in the average number of eye-gaze fixations for the control with time constraint group and the treatment group was not significant. Figure 6 shows the eye-gaze fixation counts (averaged over the three application authorization dialogs) of participants in the three groups. Figures 7 shows the total eye-gaze fixation coordinates of all participants in the three groups, over the eye-select, eye-draw, and eye-chase application's dialogs respectively.
– **Authorization Decision**
We also analyzed participants' authorization decisions on application installation dialogs which requested the social security number permission. Since there was only one application which requested the social security number permission, our dependent variable–fraction of social security number permissions denied by the participants, became a categorical variable. Therefore, we conducted a Chi-squared test on whether the social security number permissions was denied or not. The test did not show a significant difference between the number of participants who denied the

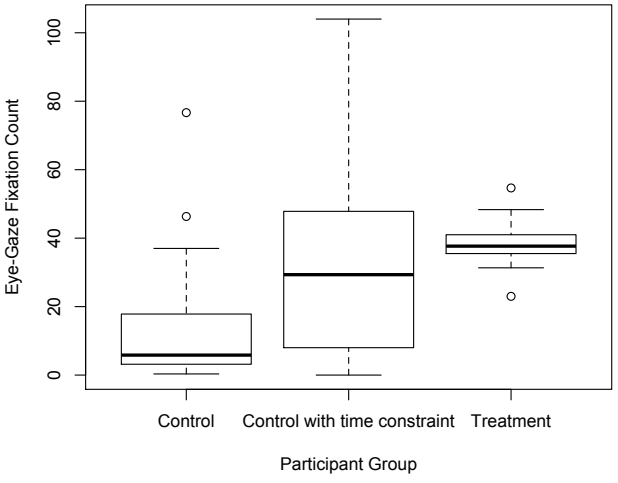
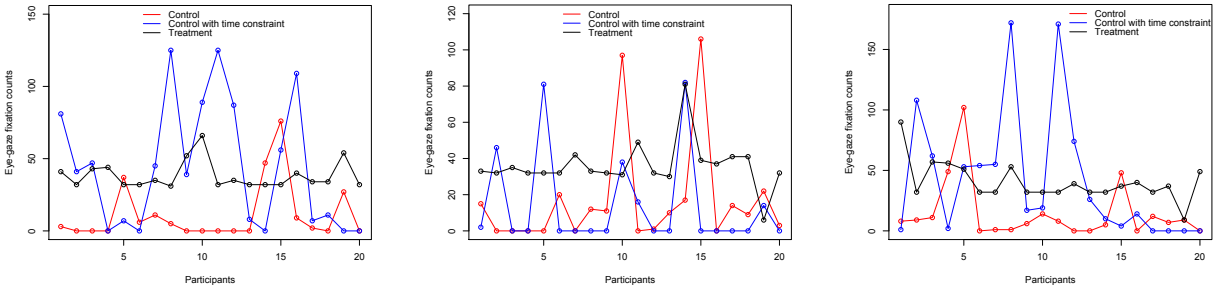


Fig. 6. Average eye-gaze fixation counts on application permissions area of interest for the control, control with time constraint, and treatment group (Attention)



(a) Eye-Select Application (b) Eye-Draw Application (c) Eye-Chase Application

Fig. 7. Eye-gaze fixations of participants on the application installation dialogs' permission area of interest (Attention)

social security number permission in the control group (mean=0, SD=0), control with time constraint group (mean=0, SD=0), and the treatment group (mean=0.15, SD=0.36) with p=0.04. 0 of the 20 participants in the control group (0%) denied the social security number permission request as compared to 0 of 20 participants in the control with time constraint group (0%), and 3 of 20 participants in the treatment group (15%).

When debriefed about the goal of the experiment, a majority of the participants reported that they had noticed the social security permission and thought it was strange that Facebook was requesting such information. However, they still authorized the permission because the experiment was being conducted in a lab environment. Although explicitly told about the option of not installing an application, some participants thought that they had to authorize all the permissions in order for the application to work.

4.2 Experiment: Habituation

Our second experiment focused on finding our approach's resistance against habituation. Our design is inspired from Bravo-Lillo et al. work on attractors for security dialogs [9, 10]. They used attractors to highlight a field that was of no value during habituation, but contained critical information after the habituation period. We adapted their design by first habituating the participants to the dialogs (randomly from eye-select and eye-draw applications) with similar and safe permissions, and then dialogs from eye-chase application containing additional SSN permission after the habituation period.

Similar to the attention experiment, we used a between-subjects design and the participants were presented with one of the three mechanisms of installing authorization dialogs.

4.2.1 Methodology

We recruited our participants through Craigslist, and word of mouth. Our study was advertised on Craigslist and the eligible candidates were invited to campus for participation. We also asked the participants to spread the word about our study without revealing the actual goal of the study.

The participants logged into their Facebook account, and were told that they would be answering a set of 30 Facebook application dialogs inside the browser, and then complete a survey. The participants were repeatedly exposed to an installation dialog of eye-select and eye-draw applications during the habituation period. These applications showed the same public profile permission on their dialog. After the habituation period of 20 dialogs concluded, we presented the participants with the eye-chase application dialog (10 times) with a dangerous permission added to the permission list, to see if participants would notice it. Our habituation experiment had the same three conditions as in the attention experiment. The participants in the time constraint group had to wait for 3 seconds on each dialog before they could make a decision, whereas the treatment group participants had to perform eye-gaze based button activation on each dialog by scanning the dialog's permission text with their eyes.

4.2.1.1 Task

We instructed the participants that they would spend approximately 2-3 minutes answering a set of 30 consecutive application installation dialogs. We informed them that we are studying how long it takes a user to answer such dialogs, in order to help us design better dialogs. The participants were also informed that eye-tracking would be performed as part of the study to check the eye-tracker's accuracy for future experiments. The participants had to go through the eye-tracker calibration procedure before beginning the task.

During the habituation period, the dialogs from eye-select and eye-draw applications were presented, which only requested access to public profile information. After the participant made a decision (install/cancel) on one dialog, the browser immediately presented the next dialog. To inform the participant of how many dialogs have been answered, a counter was displayed on top right corner of the dialog. The dialogs were mimicked as Facebook dialogs by adding the participant's name on it, and were shown centered on the screen. The habituation period of 20 dialogs was followed by a test period of 10 dialogs. However, the transition to the test period was not noticeable. Immediately after the first 20 dialogs, the participants were presented with 10 installation dialogs from eye-chase application, which had an additional dangerous permission of "social security number". These dialogs were also presented one by one. Participants who read the text in the test period ideally should have noticed the extra permission and clicked the "cancel" button.

4.2.1.2 Post Survey

After the test period concluded, we presented the participants with a questionnaire. We asked the participants to recall and type the contents of the last few presented dialogs. We used this response together with other follow-up questions to analyze our approach's resistance to habituation. After the participants completed the questionnaire, we informed them about the goal of our experiment.

4.2.1.3 Dependent Variables

We used the same dependent variables as in our attention experiment.

- Permission identification- The fraction of permissions identified correctly. The requested permissions were public profile information and social security number.
- Eye-gaze fixations- The number of eye-gaze fixations on the permission text area of an application authorization dialog. An eye-gaze fixation refers to the maintenance of visual gaze at a single location.
- Authorization decision- The fraction of social security number permissions denied by the participant.

Age	n=45	% of n
18 to 20	10	22.2%
21 to 30	26	58.3%
31 to 40	8	19.4%
50 to 60	1	2.2%
Gender		
Male	27	60%
Female	18	40%
Ethnicity		
Asian/Pacific Islander	16	35.5%
White/Caucasian	21	46.6%
Black/African-American	6	13.3%
Other/Multi-Racial	2	4.4%
Education Level		
Some college	16	35.5%
Associate's degree	6	13.3%
Bachelor's degree	14	31.1%
Master's degree	9	20%

Table 2. Participants demographics for the habituation experiment

4.2.2 Participants

We ran this experiment in parallel with the attention experiment between 1st Sept and 10th Oct 2016. A total of 45 participants completed the experiment, 15 per group. These participants were different from the participants in the other experiment. Table 2 shows our study participant demographics.

4.2.3 Results

Similar to the previous experiment, we studied our approach's resistance to habituation by conducting Kruskal Wallis test on each of the three dependent variables.

- **Permission Identification**
  First, we analyzed the percentage of participants who correctly identified the public profile information, and social security number permissions at the end of the test period. The post-survey questions asked the participants to select the permissions re-

quested by the last few applications. The Kruskal-Wallis test showed a significant difference between the number of permissions correctly identified by the control group (mean=0.6, SD=0.38), control with time constraint group (mean=0.53, SD=0.29), and the treatment group (mean=0.9, SD=0.2) with p=0.0047.

Post-hoc comparisons using Nemenyi test however only showed significant difference between the treatment and control with time constraint group with p = 0.013.

Figure 8 shows the number of participants who correctly identified one or both permissions correctly. The average number of participants who identified both permissions correctly was higher for the treatment group as compared to the other two groups.

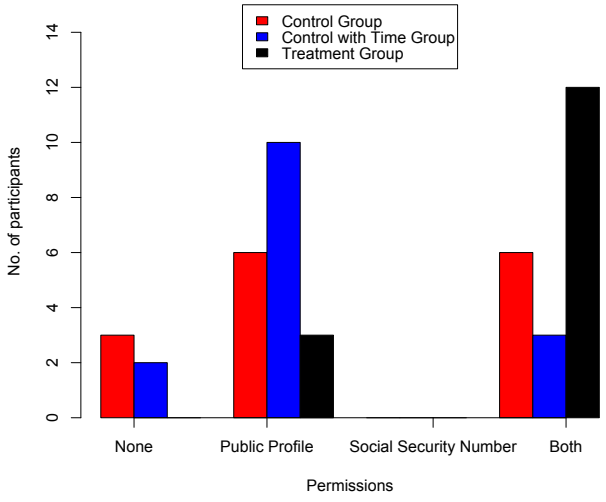


Fig. 8. Number of participants who identified one or both permissions (Habituation)

We also calculated the precision and recall for the permissions identified by the participants using the equations described in Section 4.1.4.

Figure 9 shows the permission identification precision and recall. The precision and recall was higher for treatment group as compared to the control, and control with time constraint groups.

– **Eye-Gaze Fixations**
We used eye-gaze fixation count as another metric for measuring participant's resistance to habituation. We used the same area of interest defined in our attention experiment around the permission text area and only counted the eye-gaze fixations within this area of interest. Figures 10(a) and 10(b) show the average eye-gaze fixations of all 45 participants in the control, control with time constraint, and treatment groups on the dialogs shown during habituation and test period respectively.

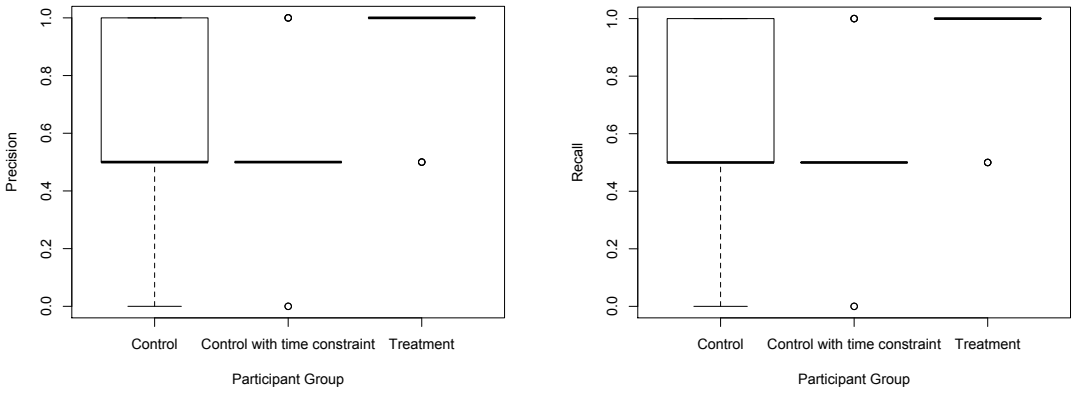
Kruskal-Wallis test on the eye-gaze fixation counts during test period showed a significant difference between the control group (mean =16.5, SD=12.74), control with time constraint group (mean=18.96, SD=16.02), and the treatment group (mean=40.26, SD= 9) with p = 0.0001. Post-hoc comparisons using Nemenyi test showed a significant difference between the number of eye-gaze fixations of the control group and treatment group with p=0.0003, and between the treatment and control with time constraint group with p=0.0013.

Figure 11 shows the average eye-gaze fixation counts of the three groups during the habituation (first two applications' dialogs) and test period (last application's dialogs).

– **Authorization Decision** Lastly, we analyzed if participants' authorization decisions are affected by habituation. For this purpose, we calculated the number of social security number permissions denied by the participants (out of 10). Kruskal-Wallis test on the fraction of social security number permissions denied did not show a significant difference between the control group (mean=0.20, SD=0.378), control with time constraint group (mean=0.293, SD=0.447), and the treatment group (mean=0.32, SD=0.526) with p=0.754.

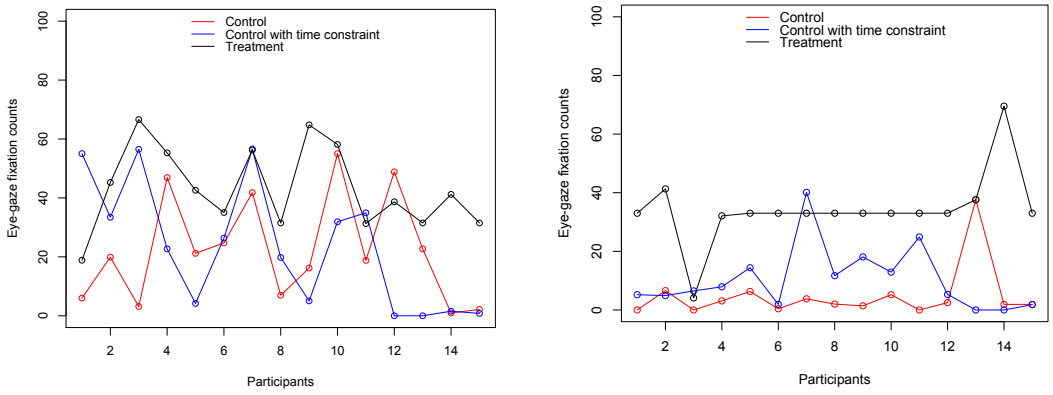
5 Discussion

Due to the requirement of staring at the dialog text, the number of eye-gaze fixations for the treatment group participants were naturally higher compared to that of the control group participants in both experiments. In order to verify that the participants actually read the permissions, we determined if they could identify which permissions were requested by the applications. The participants who used our proposed approach were able to identify both permissions (public profile, and the social security number permission) better than the other two participant groups, namely the control, control with time constraint group. Moreover, the permission recall



(a) Precision (b) Recall

Fig. 9. Participant permission identification precision and recall during habituation experiment



(a) Habituation Period (b) Test Period

Fig. 10. Eye-gaze fixations of participants on the application installation dialogs area of interest during habituation and test period

and precision was higher for the treatment group participants.

We did not observe any difference in the authorization decisions of the three participant groups. Although the participants were explicitly told that they are free to choose not to install an application, most participants mentioned that they still installed the application despite being surprised with a Facebook application requesting "social security permission" because they trusted the experimenter.

We tried to evaluate participant attention in a realistic dialog scenario; however, the validity of our experiments is still limited. The sample size of 45-60 participants per experiment is small. In future, we intend to design a larger study to examine actual behaviors, and whether users would make different choices when forced to read the dialogs, by incorporating the following:

1. Give the users the choice to install one of several different apps that vary based on the permissions requested, and see if the users would make different choices when they are forced to read the dialogs.
2. Expose the users to our proposed approach for a longer duration to analyze resistance to habituation.

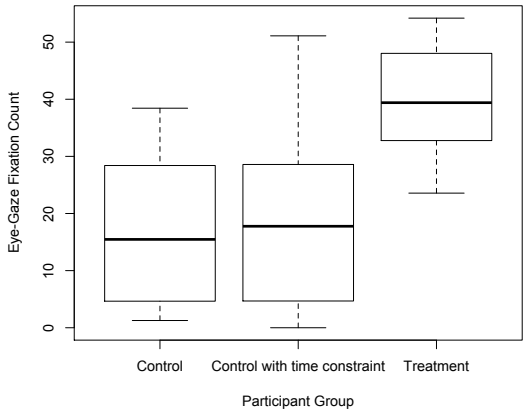


Fig. 11. Average eye-gaze fixation counts on the application permissions for the control, control with time constraint, and treatment groups (Habituation)

6 Conclusion

In this paper, we investigated the hypothesis that forcing a user to look at the application permissions will increase the probability of user paying attention and reading the permissions. Therefore, we investigated the viability of an eye-tracking based approach in enforcing user attention towards permissions, and therefore mitigating habituation. We implemented a prototype of our approach as a Chrome browser extension.

Our experiment on 60 participants showed that the participants who were forced to look at the permissions by using our extension to install the applications demonstrated a slight improvement in attention. The treatment group participants were able to better identify the requested permissions as compared to the rest of the participants. The participants' logged eye-gaze coordinates supported our hypothesis and there was a significant difference between the eye-gaze fixations of the control, control with time constraint, and treatment group participants. However, the hypothesized increase in the rate in which participants denied a dangerous/unnecessary permission, from the control groups to the treatment group was not statistically significant. This could primarily be due to the study design and it being conducted in a lab environment.

Our experiment on 45 participants showed similar results as from the first experiment, after the participants were repeatedly exposed to a set of application dialogs. The participants who were forced to look at the permissions were able to better identify requested permissions correctly as compared to the control group participants, with higher precision and recall. The participants' logged eye-gaze coordinates on the dialogs presented during the test period showed that there was a significant difference between the eye-gaze fixations of the three participant groups. Once again, the hypothesized increase in the rate in which participants denied a dangerous/unnecessary permission, from the control groups to the treatment group was not statistically significant. There was no difference in the fraction of social security number permissions denied by the three groups.

References

[1] Do you need mobile antivirus software? http://www.androidauthority.com/do-you-need-mobile-antivirus-software-663034/.

[2] The eye tribe tracker. https://theeyetribe.com.

[3] Facebook security issue: Facebook color scam, back again. https://developers.facebook.com/docs/facebook-login/login-flow-for-web/v2.2.

[4] The 'most used words' facebook quiz app accused of data stealing. http://www.forbes.com/sites/amitchowdhry/2015/11/29/the-most-used-words-facebook-quiz-app/#73c615c14bb6.

[5] Facebook login flow. http://www.cmcm.com/blog/2014-08-07/348.html, 2014.

[6] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. How polymorphic warnings reduce habituation in the brain–insights from an fmri study. In *CHI. ACM*, 2015.

[7] M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila. Comparative eye tracking of experts and novices in web single sign-on. In *Proceedings of the third ACM conference on Data and application security and privacy*, pages 105–116. ACM, 2013.

[8] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *SOUPS*, 2010.

[9] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper. Harder to ignore? revisiting pop-up fatigue and approaches to prevent it. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 105–111, Menlo Park, CA, July 2014. USENIX Association.

[10] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 6:1–6:12, New York, NY, USA, 2013. ACM.

[11] P. H. Chia, Y. Yamamoto, and N. Asokan. Is this app safe?: a large scale study on application permissions and risk signals. In *Proceedings of the 21st international conference on World Wide Web*, pages 311–320. ACM, 2012.

[12] S. Egelman. My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2369–2378. ACM, 2013.

[13] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 3. ACM, 2012.

[14] S. Furman and M. Theofanos. Preserving privacy–more than reading a message. In *Universal Access in Human-Computer Interaction. Design for All and Accessibility Practice*, pages 14–25. Springer, 2014.

[15] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 2647–2656, New York, NY, USA, 2014. ACM.

[16] M. J. Kalsher and K. J. Williams. Behavioral compliance: Theory, methodology, and results. *Handbook of warnings*, pages 313–329, 2006.

[17] D. Miyamoto, T. Iimura, G. Blanc, H. Tazaki, and Y. Kadobayashi. Eyebit: Eye-tracking approach for enforcing phishing prevention habits. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, pages 56–65. IEEE, 2014.

[18] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos. Frappe: detecting malicious facebook applications. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, pages 313–324. ACM, 2012.

[19] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Android permissions: A perspective combining risks and benefits. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies*, SACMAT '12, pages 13–22, New York, NY, USA, 2012. ACM.

[20] E. Steel and G. A. Fowler. Facebook in privacy breach. http://www.wsj.com/articles/SB10001424052702304772804575558484075236968, Oct. 2010.

[21] T. Whalen and K. M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, GI '05, pages 137–144, School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 2005. Canadian Human-Computer Communications Society.

A Survey Questions (Attention Experiment)

The participants were asked to answer the following questions at the end of the experiment.

A.1 Eye-Tracking Experience

Please answer the following questions about your eye-tracking experience where 1 represents Poor and 5 represents Excellent.

1. Rate your over-all experience with eye-tracking
2. Rate the accuracy of eye-tracking during application installation tasks
3. Rate the accuracy of eye-tracking during the eye-draw task
4. Rate the accuracy of eye-tracking during the image selection task

A.2 Content Recall and Permission Identification

You were presented with three installation windows during this study

1. Eye Chase Application Installation Window (image added)

   Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none":
2. Eye Draw Application Installation Window (image added)

   Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none":
3. Eye Select Application Installation Window (image added)

   Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none":
4. Did any of the above installation windows request permissions to your information?
   - Yes
   - No
   - I Don't Know
5. If you answered yes to the previous question, which permission(s) did these installation windows request. Select all that apply
   - Public profile information
   - Phone number
   - Social Security Number
   - Photos
   - Mother's maiden name

6. On most of the installation windows you saw, did you intentionally read the text in the installation window?
   - I ignored it
   - I tried to read a little
   - I read every word
7. On the last installation window you saw, did you intentionally read the text in the installation window?
   - I ignored it
   - I tried to read a little
   - I read every word

A.3 Demographics

1. What is your gender?
   - Female
   - Male
2. What is the highest level of education you have completed?
   - Some high school
   - High school/GED
   - Some college
   - Associate's degree
   - Bachelor's degree
   - Master's degree
   - Doctorate degree
   - Law degree
   - Medical degree
   - Trade or other technical school degree
   - Decline to answer
3. What is your age?
   - 18-20
   - 20-30
   - 30-40
   - 40-50
   - 50-60
   - 60 and above
4. What is your race/ethnicity?
   - Asian/Pacific Islander
   - Black/African-American
   - White/Caucasian
   - Hispanic
   - Native American/Alaska Native
   - Other/Multi-Racial
   - Middle East
   - Decline to answer

B Survey Questions (Habituation Experiment)

The participants were asked to answer the following questions at the end of the experiment.

B.1 Content Recall and Permission Identification

1. The image below corresponds to one of the dialogs you saw during this study:
   (image added)
   Please type in the contents of the most-recently shown dialog, to the best of your memory. If you have no memory, please type "none"
2. What did the last dialog you saw communicate
   - The quality of my performance in the study
   - The application requires access to public profile information and social security number
   - The amount of money I will be paid for the study
   - The application requires access to public profile information and photos
   - I'm not sure
3. During most of the dialogs you saw, did you intentionally read the text inside them?
   - I ignored it
   - I tried to read a little
   - I read every word
4. During the last dialog you saw, did you intentionally read the text inside it?
   - I ignored it
   - I tried to read a little
   - I read every word

B.2 Demographics

Similar to the previous experiment