Preserving Privacy – More Than Reading a Message

Susanne Furman and Mary Theofanos

National Institute of Standards and Technology, 100 Bureau Drive,
Gaithersburg, Maryland, 20899, USA
{Susanne.Furman,Mary.Theofanos}@nist.gov

Abstract. Social media has become a mainstream activity where people share all kinds of personal and intimate details about their lives. These social networking sites (SNS) allow users to conveniently authenticate to the third-party website by using their SNS credentials, thus eliminating the need of creating and remembering another username and password but at the same time agreeing to share their personal information with the SNS site. Often this is accomplished by presenting the user with a dialog box informing them that they will be sharing information. We were interested in determining if SNS users authenticating to a third-party website with their SNS credentials, were reading the informational message and if changing the message format would impact the choice to continue or cancel. Format type did not alter the participant's choice to continue. Eye-tracking data suggests that the participants who chose to continue read some of the words in the message.

Keywords: Access to the Web, privacy, eye tracking, authentication.

1 Background

By creating an identity on a website, users gain the ability to engage in a wide range of activities like e-mail, online shopping and banking, or in social networking activities. Today's Web is very site-centric where the user is expected to maintain a separate copy of their username and corresponding password for each site they join [14]. To create and maintain these separate identities, users must create and remember their usernames and passwords; populate a profile often with the same data across sites; and remember each site's different password rules [9].

Federated identity management offers the user a solution to reduce the burden of multiple identities. It provides a technology that websites can offer to users as a single sign-on (SSO) experience. SSO offers the user an easier experience through a more consistent and less frequent log-on process. The user can authenticate once and access their protected resources across multiple websites [9].

Facebook[1] offers its users a type of SSO that allows users to connect their SNS identity, friends, and personal information to any site that offers this service.

[1] Disclaimer: Any mention of commercial products is for information only; such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best for the purpose.

C. Stephanidis and M. Antona (Eds.): UAHCI/HCII 2014, Part IV, LNCS 8516, pp. 14–25, 2014.

Through this technology, a user's SNS ID becomes a gateway that provides access to the digital world. The third-party website offering this service benefits through distributing their services with minimal effort to SNS users and the SNS users benefit by eliminating the cumbersome process of registering, and creating and remembering a username and password [8].

Social media has become a mainstream activity where people share all kinds of personal and intimate details about their lives; photos of their children, family and friends; their email address; and even their physical location. Many of these users are unaware that both their personal information as well as that of their friends is passed to these third parties when they authenticate using their SNS credentials.

SNS websites do inform users (through a pop-up dialog window) that authentication to a third-party website using their SNS credentials results in their personal information being shared with the website. The user is typically given the option to agree to or cancel the authentication request.

Privacy advocates are concerned that these SNS authentication services pose new sets of concerns about how data are collected and shared among websites. One major concern is that because users don't completely understand how these services work and have the mistaken impression that their data isn't being collected [8].

Many popular SNS applications transmit users' identifying information to dozens of ad and internet tracking companies. This practice affects millions of SNS application users, even those who implement the strictest privacy settings. Ten of the most popular applications reviewed transmitted not only a user's ID and personal information but also personal information about the user's friends to outside companies [13]. Approximately 850 million times per month, apps have asked SNS users to release their basic information [17].

Most SNS do not make it clear exactly what user information is shared and to whom it is given, so many SNS users make the assumption that their information is safe [12]. Also, SNS privacy settings are often difficult to manage and users often do not change them from their defaults, which are generally set to maximize the visibility and sharing of users' profile information [7].

So, it is not surprising that SNS users are unaware of and don't understand the privacy dangers from data sharing with third-party apps or websites that they connect to using their SNS accounts. Many users believe that online communities are safe and don't understand privacy policies [16]. They do not realize the extent to which they share not only their own information, but that of their friends as well [2]. As a result, they feel their risk of unwilling or inadvertent disclosure of personal information is very low [15].

Motivation is directly tied to attention so the more motivated a person is to perform a particular task, the more effort and attention they will devote [3]. Authentication tasks (i.e., entering a username and password) or privacy and security tasks (e.g., reading a privacy policy) are not considered primary tasks but are viewed as secondary and a requirement for completion of primary tasks.

Another factor impacting attention is that often security messages resemble other non-essential pop-up dialogs. As a result users often fail to realize that they contain important information about how their privacy and security will be affected by taking a certain action. Often users disregard or do not read these dialogs and only click "Agree" or "OK" to close the dialog message [18].

Message format can also impact reading. Information presented in a list format can benefit users who are searching for information that is embedded in other text. List formats facilitate easier information acquisition than paragraph formats, due to their lower print density [19]. The results of a 1995 study demonstrated that older patients were better able to find, understand, and later recall medication instructions that were presented in list format rather than paragraph format [10].

2 Research Goal

Millions of SNS users are utilizing their SNS identities to authenticate to third-party websites. Many are unaware that both their personal information and that of their friend's is passed to these third parties. SNS websites typically inform the user via a dialog message in a pop-up window that by agreeing they will be sharing personal data with the third-party website. However, the user does have the option to agree or cancel the authentication request.

We wanted to investigate if users read the authentication dialog message explaining that their personal information would be shared with a third-party website. Also we wondered if manipulating the format of the dialog message (i.e., sentence-style, list-style, and list with personal data displayed) would impact whether participants would decide to continue with the authentication process. Previous research testing message formats explains the lack of observable effects by claiming that participants did not read or were habituated to the dialog messages. The study supported this explanation with screen capture videos that show the message was displayed for a period of time but clarifies that without an eye tracker they could not be certain users read the message [5]. Specifically we were interested in:

- Will SNS users authenticate to a third-party website using their SNS credentials after being informed that their personal information will be shared with the website?
- Will manipulating the format of the dialog message (i.e., sentence-style, list-style, and list with personal data displayed) influence a participant's choice to continue with the authentication process? Figure 1 shows the three formatted messages.
- What information does the eye-gaze data show about the content participants viewed in the dialog message if any? Does the format of the message make any difference in a participant's authentication choice to continue?

Fig. 1. Format message conditions

3 Methodology

3.1 Participants

A study was conducted at NIST for a period of four weeks to examine these three message conditions. Participants were required to have an SNS account and received $50 for participation in a 30 min session.

Of the 120 participants initially recruited, 117 completed the study. One participant withdrew, and hardware malfunctions prevented two others from completing the study. Participants ranged in age from 17 to over 60 and age groups were fairly equally represented. There were fewer males (35 %) than females (65 %). Most of the participants (92 %) had at least some college experience.

3.2 Instruments and Apparatus

Software code was written to intercept and replace the original SNS authentication message dialog. The code replaced the original dialog message with a similar message in one of three formats identified above. Participants were randomly assigned to one of the three format conditions at the start of their session.

The study used a PC integrated with the Tobii T60XL[1] eye tracker paired with a high-resolution 24" TFT wide screen monitor having a display pixel resolution of 1900 x 1200. The eye tracker looked like a normal computer display, and its high resolution cameras were invisible to the participant. The online version of the Wall Street Journal (WSJ.com website)[1] was shown in Internet Explorer 9. All precision measurements were done at 60 Hz sampling rate, and all participants completed a nine point eye calibration prior to the start of the session. Gaze data was logged by Tobii Studio software.

3.3 Sessions

After signing the consent form, participants logged into their SNS account. The researcher started the intercept software, assigned the participant to one of the three format conditions, and started the eye-tracking device. The intercept software launched the online version of the third-party website. The researcher asked participants to find a news story of interest, and once selected, the researcher provided the following scenario:

> You are sitting at home and are very interested in reading this news story but you don't have time right now. Given the number of times that news sites refresh their content, you are concerned that you may not find the story when you come back. Please save the news story so that you can read it later.

The researcher instructed the participant to do whatever they would do at home. Saving the news story on the site required the participant to set up an account or use their SNS credentials to authenticate to the third-party website.

If the participant chose not to use their SNS credentials to authenticate, the researcher stopped the eye tracker and instructed them to complete an online survey about their SNS use and privacy concerns. If the participant chose to use their SNS credentials to authenticate, the choice was recorded, the eye tracker captured the participant's interaction with the dialog message, and particpants completed the online survey.

After session completion, the researcher logged the participant out of their SNS account, removed the intercept application from their SNS apps, asked if there were any questions, and thanked the participant for their time. Participants were compensated for their time prior to leaving the laboratory.

4 Results

4.1 Authentication Using SNS Credentials

The participants were randomly assigned to one of the format conditions at the start of their session resulting in 40 participants in the sentence-style format, 38 in the list,

and 39 in the list with data displayed formats. Fifty-nine (51 %) of the 117 participants chose to use SNS credentials to authenticate to the third-party website.

Of the 40 participants in the sentence-style format, 23 (58 %) authenticated using their SNS credentials; of the 38 participants in the list-style, 17 (45 %) authenticated; and of the 39 in list with data format, 19 (49 %) authenticated. A chi squared test was performed to determine whether the format conditions were equal with respect to authentication choice. Although there were more participants using their SNS credentials to authenticate in the sentence-style format, use/did not use data comparing the three conditions were not significant, χ^2 (2, N= 59) = 1.3382, p > 0.5.

4.2 Eye-Tracking Data

Tobii Studio software captured the gaze data as participants viewed the third-party website. Of particular interest was where participants allocated their visual attention when the SNS SSO dialog box appeared. For that reason, only those participants who chose to use their SNS credentials and those who started to use their SNS credentials but did not continue were included in the eye-tracking analyses.

AOI 1 – Dialog Message Analyses. An area of interest (AOI) is a user-defined area on the stimulus that is used for capturing and analyzing the eye-tracking data (see Figure 2). The message content, title, and action buttons on the SNS authentication dialog message were marked as the initial AOI. Of particular interest was the amount of attention the AOI received. Therefore, the mean and standard deviations were calculated for the following metrics: (1) fixation count: the number of times the participant fixates or pauses over areas of interest - this indicates how many times the participant looks at the area; (2) total fixation duration: measures the sum of the length of time for all fixations or pauses within an AOI measured in seconds; (3) total visit duration: how much time in seconds the participant spent within an area of interest - this indicates the level of the participant's involvement with the area. The overall mean total visit duration was 5.56 s. Participants in the list format condition spent less time viewing the AOI than those in the sentence-style or list with data displayed format conditions. Individuals who chose not to connect had the longest total visit duration. Table 1 shows the total visit duration, fixation counts, and fixation duration means and standard deviations across format conditions.

The mean fixation count for all participants was 21.04 fixations. The mean fixation count showed similar results with the sentence-style format having fewer fixations than the list or the list with data displayed formats. However, the participants who did not choose to connect had the most fixations.

The mean fixation duration for all participants was 4.39 s. The results across format condition show that the participants in the sentence format condition spent less time fixating within the AOI than the list format participants.

Table 1. AOI total fixation, fixation count, and total fixation duration (seconds) mean and standard deviations across format condition

Format Condition	Total Visit Duration(s)		Fixation Count		Fixation Duration(s)	
	Mean	*St Dev*	Mean	*St Dev*	Mean	*St Dev*
Sentence-style	4.85	*4.35*	16.75	*14.11*	3.28	*2.78*
List	4.70	*3.74*	17.8	*11.16*	3.59	*3.97*
List with Data	8.07	*6.42*	26.67	*21.8*	6.16	*5.1*
Did Not Connect	13.01	*5.94*	31	*16.02*	6.03	*2.6*

Multiple AOI Analyses. We separated the dialog box into separate AOIs, including the basic information area (e.g., name, email, gender), the profile picture, and the participant's photos of friends. The sentence-style format did not include any shared photos and is not included in these analyses.

The main content AOI included the personal information that the participants shared from their profile. Participants spent less time fixating within the list format AOI than within the AOIs in the sentence-style, and the "did not connect" format conditions.

The list format had fewer fixations than the sentence-style format, list with data format and didn't connect format groups. They also had a shorter visit duration than the sentence-style format, list with data format, and didn't connect format conditions. Table 2 shows the fixation duration, fixation count, and total visit duration means and standard deviations across format conditions.

Table 2. Multiple AOI total fixation duration, fixation count, and total fixation duration means and standard deviations

Format Condition	Total Visit Duration (s)		Fixation Count		Fixation Duration (s)	
	Mean	*St Dev*	Mean	*St Dev*	Mean	*St Dev*
Personal Information Message Content						
Sentence	1.95	*2.53*	8.93	*10.17*	1.63	*2.19*
List	1.66	*1.64*	7.25	*6.21*	1.45	*1.37*
List with Data	4.13	*4.82*	17	*19.93*	3.68	*4.44*
Did Not Connect	6.85	*3.38*	18.6	*11.59*	3.6	*1.79*
Photos of Friends						
Sentence	*Did not have photos on their message dialogs*					
List	.75	*.56*	3.83	*2.17*	.62	*.55*
List with Data	1.47	*1.25*	4.86	*3.44*	1.32	*1.25*
Profile Photo						
Sentence	.61	*.13*	3.33	*.58*	.58	*.16*
List	.21	*.13*	1.25	*.05*	.21	*.13*
List with Data	.38	*.21*	2.33	*1.53*	.38	*.21*

Large within group standard deviations precluded significant results for any pairwise comparisons, but there appeared to be a trend in the data across formats. A trend analysis attempts to spot a pattern or trend in the data. A Likelihood ratio test was conducted and showed a significant monotonic trend for fixation count and total visit duration for both the dialog box AOI and personal content AOI, $p < 0.05$. This was also the case for the fixation count for the dialog AOI.

A heat map was created to visualize the eye-tracking data (see Figure 2). The heat maps were consistent with the eye-tracking data and showed that the majority of participants did read some of the content of the dialog message that indicated their personal information would be shared with the third-party website.

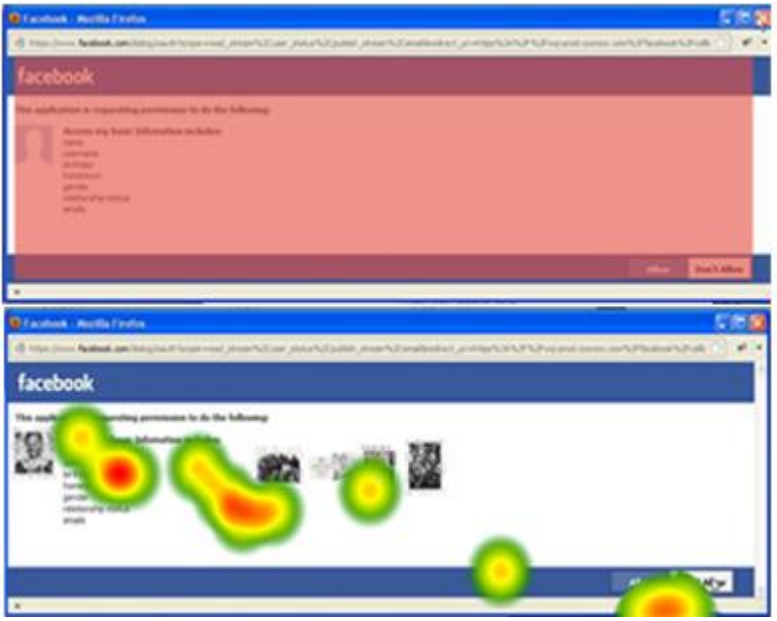

Fig. 2. AOI and heat map example

Survey Responses. Our online SNS use and privacy survey data shows that 57 % of the 117 participants change their SNS privacy settings once a year and approximately 80 % of those individuals set the level at strict or extremely strict where only their friends can see their information. The majority of participants were very concerned about having their cell phone (91 %), postal address (91 %), email address (78 %), and picture (64 %) shared with a third-party website without their permission. That concern does not appear to transfer to SNS accounts where the respondents are willing to share their name (83 %), gender (80 %), birthday (61 %), picture (72 %), interests (71 %), friends (64 %), current city (65 %), and education (66 %).

5 Discussion

We asked participants to save a news story they selected from a third-party website requiring authentication either by setting up an account or using their SNS credentials. Approximately half of the participants chose to use their SNS credentials to authenticate to the third-party website.

We hypothesized that participants who were presented with the list with data format would spend more time reading the dialog box than the other formats. Unfortunately the standard deviations precluded finding any significant differences for pairwise comparisons. However, we did see a trend showing that there is a significant increase in reading times across the formats. We also hypothesized that these participants upon seeing their personal information displayed would cancel authentication. While these participants spent more time reading the dialog message, they did continue with authentication.

One might assume with eye-tracking data that there is a relationship between what the participant is looking at and what they are thinking about. Unfortunately this isn't necessarily true. What eye tracking provides is an objective way of determining where the participant's visual attention is located. Our data showed that most of the participants using their SNS credentials actually read some part of the message dialog pop-up informing them that their personal information would be shared.

College students read about 300 words per minute with an average of 200 microseconds per word [19]. The dialog box for the sentence-style format contained about 30 words, while the other formats were dependent on the information the participant displayed in their profile. Word processing in text is reflected in fixation time where short, regularly spelled, frequent in occurrence, and semantically/syntactically predictable words are fixated for a shorter period of time. Words that are predictable are often skipped, and better readers average about 84 fixations per 100 words, often skip more words, and have shorter fixations [11].

The total mean visit duration across format conditions was approximately eight seconds, giving the participants enough time to read approximately 10 words and the content was also predictable. The mean fixation count across formats was 23 accounting for approximately 19 words which leads us to believe that participants read the content in the dialog box.

6 Conclusions

Our eye-tracking data shows that participants read content in the SNS authentication dialog message box but also continued with authentication even though they were informed their personal information was about to be shared. Although this does not indicate they processed any of the words or content, it does seem to suggest that they did not habituate to the dialog box or just select the agree button to close the dialog so that they could continue with their main task.

There was a signficant trend in reading times across formats. But the format style did not impact participants' decision to continue with authentication. Participants chose to share their personal information by selecting to 'allow' the SNS to authenticate to the third-party website.

Participants comments were inconsistent with their actions. Participants admit to sharing many types of personal information on their SNS pages but are more concerned with sharing personal information with others (e.g., ad companies or marketers). They were adamantly opposed to sharing their personal information with a third-party website without their consent. Even though participants gave consent, they didn't seem to realize that their SNS privacy settings did not apply to the sharing of their personal information when they authenticated using their SNS credentials.

Some researchers think that the SNS authentication message is too generic and does not adequately convey this data sharing. They believe that users do not realize they share so much information with these third-party websites and applications [2]. While others believe that the average user is reacting to these interruption dialog messages with responses that range from mild irritation to annoyance, and users quickly learn to visually and cognitively dismiss them [1]. Still others think that over the years, users are trained to click dialogs away to complete the primary task. Because these interception dialogs interrupt the user's primary task, the users do not bother to read them and as a result, do not heed warnings [4].

Our participants may not have fully understood the risks associated with innocent-appearing disclosure of information like their hometown or current city. As we are quite aware, users' attention is scarce, and identity management is seldom a user's primary goal. The participants in our study may have quickly scanned the message and did not fully understood what they were consenting to. Or quite simply, our participants may have continued authentication even though they were informed that their personal information was being shared because they believed the third-party website to be a reputable site that would protect their information.

Having a single sign-on method such as SNS identity eases the burden for users trying to authenticate to a new online service. Often users are willing to trade-off some possible or unknown risks for the convenience of not having to set up another account, and create and remember another username and password [6]. The Federal Trade Commission and others have policy goals of adequately informing users of when their personal information might be shared. Future research should explore other types of alerts and explore whether users understand the potential implications and consequences of their choices.

References

1. Bahr, G.S., Ford, R.A.: How and why pop-ups don't work: Pop-up prompted eye movements, user affect and decision making. Computers in Behavior 27(2), 776–783 (2010)
2. Besmer, A., Lipford, H.R.: Users' (mis)conceptions of social applications. In: Mould, D., Noël, S. (eds.) Graphics Interface, pp. 63–70. ACM, New York (2010), `http://hci.uncc.edu/pubs/Misconceptions.pdf` (retrieved)

3. Bitgood, S.: The role of attention in designing effective interpretive labels. Journal of Interpretation Research 5(2), 31–45 (2000), http://www.jsu.edu/psychology/docs/5.1-role_of_attention.pdf (retrieved)
4. Bohme, R., Kopsell, S.: Trained to accept?: a field experiment on consent dialogs. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, pp. 2403–2406. ACM (2010)
5. Egelman, S.: 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, pp. 2369–2378. ACM (2013)
6. Good, N.S., Grossklags, J., Mulligan, D.K., Konstan, J.A.: Noticing notice: a large-scale experiment on the timing of software license agreements. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 607–616. ACM (April 2007)
7. Gross, R., Acquisiti, A.: Information revelation of the privacy in online social networks. In: Proceedings of the 2005 ACM Workshop on Privacy in Electronic Society, pp. 71–80. ACM, New York (2005), doi:10.1145/1102199.1102214
8. Ko, M.N., Cheek, G.P., Shehab, M.: Social-networks connect services. Computer 43(8), 37–43 (2010), doi:10.1109/MC.2010.239; MacMillan, D.: FB connect: Your 8,000 hidden friends. Bloomburg BusinessWeek: Technology (April 2, 2009) http://www.businessweek.com/technology/content/apr2009/tc2009041_649562.htm (retrieved)
9. Maler, E., Reed, D.: The venn of identity, options and issues in federated identity management. IEEE Security & Privacy 6(2), 16–23 (2008), doi:10.1109/MSP.2008.50
10. Morrow, D., Leirer, V., Altieri, P.: List formats improve medication instructions for older adults. Educational Gerontology: An International Quarterly 21(2), 151–166 (1995), doi:10.1080/0360127950210204
11. Rayner, K., Juhasz, B.J., Pollatsek, A.: Eye Movements During Reading. In: Snowling, M.J., Hulme, C. (eds.) The Science of Reading: A Handbook, pp. 79–97. Blackwell Publishing Ltd., Oxford (2008), doi:10.1002/978047-757642.ch5
12. Roberts, K.K.: Privacy & perceptions: How facebook advertising affects its users. The Elon Journal of Undergraduate Research in Communications 1(1), 24–34 (2010), http://www.elon.edu/docs/e-web/academics/communications/research/03RobertsEJSpring10.pdf
13. Steel, E., Fowler, G.A.: Facebook in privacy breach: Top-ranked applications transmit personal IDs, a journal investigation finds. The Wall Street Journal (October 17, 2010), http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html (retrieved)
14. Sun, S.T., Boshmaf, Y., Hawkey, K., Beznosov, K.: A billion keys, but few locks: The crisis of web single sign-on. In: Proceedings of the 2010 Workshop on New Security Paradigms, pp. 61–72. ACM, New York (2010), doi:10.1145/1900546.1900556
15. Tow, W., Newk-Fon, H., Dell, P., Venable, J.: Understanding information disclosure behavior in Australian Facebook users. Journal of Information Technology 25(2), 126–136 (2010), doi:10.1057/jit.2010.18
16. Tuunainen, V.K., Pitkanen, O., Hovi, M.: Users' awareness of privacy on online social networking sites – case Facebook. In: BLED 2009 Proceedings (Paper 42) (2009), http://aisel.aisnet.org/bled2009/42 (retrieved)

17. Wang, N., Xu, H., Grossklags, J.: Third party apps on facebook: Privacy and the illusion of control. In: Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (Article No. 4), ACM, New York (2011), doi:10.1145/2076444.2076448
18. West, R.: The psychology of security. Communications of the ACM 51(4), 34–40 (2008), doi:10.1145/1330311.1330320
19. Wolgater, M.S., Shaver, E.F.: Evaluation of list vs. paragraph text format on search time for warnings symptoms in a product manual. Advances in Occupational Ergonomics and Safety 4, 434–438 (2001)