Do Password Managers Nudge Secure (Random) Passwords?

Samira Zibaei
Ontario Tech University

Dinah Rinoa Malapaya
Ontario Tech University

Benjamin Mercier
Ontario Tech University

Amirali Salehi-Abari
Ontario Tech University

Julie Thorpe
Ontario Tech University

Abstract

Passwords are the most popular authentication method due to their simplicity and widespread adoption. However, the prevalence of password reuse undermines its security. A promising strategy to mitigate the risks of password reuse is to use random passwords generated and stored by password managers, yet many users do not use them. Many web browsers have built-in password managers that employ *nudges* at the time of password creation. These nudges aim to persuade the selection of more secure random passwords; however, little is known about which designs are most effective. We study ($n = 558$) the efficacy of nudges used by three popular web browsers: Chrome, Firefox, and Safari. Our results suggest Safari's nudge implementation is significantly more effective than the others at nudging users to adopt a randomly generated password. We examine factors that may contribute to the adoption of randomly generated passwords, reasons that people adopt a randomly generated password (or not), as well as discuss elements of Safari's nudge design that may contribute to its success. Our findings can be useful in informing both future password manager nudge designs and interventions to encourage password manager use.

1 Introduction

Authentication with passwords, despite its security [14, 52] and memorability [21, 38] shortcomings, remains widespread with applications such as online banking, e-commerce, personal devices, servers, etc. The average person is estimated to have at least 26 accounts [38] and possibly more than 100 accounts [1]. The burden of remembering many passwords often leads users to rely on insecure coping methods [33], such as using the same, simple, or similar passwords [48]. To prevent these insecure coping mechanisms, password managers have become an instrumental tool for storing and generating random, complex passwords to assist users with password security and memorability. The passwords generated by password managers are expected to be less vulnerable to credential stuffing [50]—a serious concern due to password leaks [18]—and to password guessing attacks [54]. However, password managers have not fully delivered their security promises in practice [5, 39].

Password managers, despite being recommended by security experts [20], are still not adopted by many users [39, 48]. Even when people make use of password managers, only a minority use the random password generation feature that enables its secure use [39]. One might wonder how to further encourage users to adopt password managers and also to accept randomly generated passwords as their password. One potential promising solution is *nudging* techniques [16] to influence adoption of password managers and their security features (e.g. randomly generated passwords) without limiting user choices [29]. While nudging has been explored in human-computer interaction [9] and some computer security contexts [58], research on nudging in the context of adopting password managers or their security features (e.g., randomly generated passwords) is sparse.

In this paper, we initiate studying the effect of nudging on the adoption of security and storage features of password managers. In particular, we explore how effective current browser-based password managers are at nudging users to adopt their randomly generated passwords and storage features. We also aim to gain a deeper understanding of why people choose to adopt generated passwords (or not). Our specific research questions are:

*Contact author: Samira Zibaei <samira.zibaei@ontariotechu.ca>.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

Q1 How do the three most popular browser-based password managers (Chrome, Firefox, and Safari) compare to each other in nudging users to adopt randomly-generated passwords?

Q2 Does the complexity of a website's password policy contribute to the adoption rate for randomly generated passwords?

Q3 What factors contribute to the adoption rate for randomly generated passwords and saving passwords in the password manager?

Q4 What are the rationales of users to (not) adopt a randomly generated password?

To investigate these questions, we conducted a user study ($n = 558$) to evaluate the effectiveness of the generated password nudges employed by Chrome, Firefox, and Safari. Participants were asked to register for a new website, so we can observe their interaction with the password managers. Following registration, participants complete a questionnaire that asks their reasons for adopting the generated password (or not). Our website assigned participants one of two password policies (1C8 and 3C12)[1] to evaluate its impact on users' decisions when confronted with simple or complex password requirements. We perform both quantitative and qualitative analyses on our collected statistics and participant's free-form comments regarding their use of the randomly generated password during their account registration.

Our contributions and findings include: (i) Analysis of which browser password manager nudges are most effective. We discuss differences between the nudge designs of the password managers we study, and possible reasons for our findings, which can be useful in informing future password manager nudge designs. (ii) Identification of a number of factors that influence users' decision to adopt a randomly generated password, such as previous use of a password manager, former familiarity/use of a generated password, and whether they noticed the nudge. (iii) Investigation of reasons why people believe they did (not) use the generated password. This information can also be useful in informing both future password manager nudge designs and interventions to encourage password manager use.

The paper is structured as follows. Section 2 discusses previous work that relates to our research. Section 3 elaborates on the purpose of our study, how we recruited our participants, our study's structure, how we collected our data, statistical testing methods, and qualitative analysis methods employed. The results of our study are presented in Section 4, as well as participant demographic information. We discuss the results and limitations of our study in Section 5, and conclude in Section 6.

[1] 1C8 is a password policy that only requires a minimum of 8 characters. 3C12 is a password policy that requires a minimum of 12 characters and at least 3 character classes. Character classes include lowercase characters, uppercase characters, special characters, and numbers.

2 Related Work

We first briefly review password shortcomings, then discuss related work on password managers and nudging.

Many passwords to manage. Passwords remain the most popular authentication method for computer systems [8]. Unfortunately, with the proliferation of online services, the number of passwords that each user needs to remember has increased exponentially. The average person has between 70–80 passwords [56]. Creating strong, unique, and complex passwords that are easy to remember is an unavoidable challenge for users. As a result, users resort to making weak passwords that are easy to remember (sometimes, with their personal information) or reuse their passwords for multiple accounts [15, 31]. Both of these practices yield lower security. With password reuse, the leak of a password from one account renders other potentially high-risk accounts vulnerable [48]. Passwords with personal information are more vulnerable to guessing attacks [54]. Also, recently many advances have been made towards more effective guessing attacks, which leverage the reoccurring password patterns in large-scale leaked password datasets and machine learning techniques [22, 25, 32, 35, 36, 53, 54].

Password managers and usability. Password managers can generate, store, and remember random passwords for users to enhance their password security. Several usability issues have been reported in studies conducted on password managers such as poor user interface design [3] and lack of important functionalities (e.g., recovering changed or deleted credentials) [5]. It is shown that the use of technical terms when describing features (e.g., "password generator") makes password managers seemingly complicated for users [47]. Recently, a cognitive walkthrough indicated some features of password managers (e.g., autofill, user interface design, and linking credentials to multiple sites) might help foster their adoption [46]. Some attempts have been made to improve overall usability of password managers by minimizing the user's action and enhancing their user interfaces [7, 49].

Adoption of password managers. The adoption of password managers has faced challenges beyond their usability issues. The low adoption rates of password managers is blamed on the lack of: user's trust [5, 45] in this technology, willingness to be dependent on technology [41], and awareness of its benefits [12, 45]. Convenience is yet another reason found for users not using password managers [24]. Other research found that a barrier to password manager adoption was not having enough accounts to protect, believing their accounts are not valuable enough to require using a password manager, lack of accessibility of passwords on multiple devices, and concern of the password manager's single point of failure [39]. Older adults (above 60) were found to have low adoption of password managers due to concerns about where their password is stored, and whether others might have access

to their accounts [41]. Also, impediments to adoption of standalone password managers include users not having time to install the software [6], not understanding the sense of its urgency [6], or being unwilling to hand over the control of their own passwords [10]. Other research indicates that cybersecurity knowledge is an important factor in the adoption of a password manager [5].

Adoption of randomly generated passwords. The low adoption of randomly generated passwords from password managers is a concern, which has downgraded the potential security impact of password managers. The under-deployment of randomly generated passwords might be due to a lack of awareness, interest, or trust [45]. Pearman et al. [39] in an interview study ($n = 30$) found that only one out of 12 participants who used a "built-in" or browser-based password manager adopt randomly-generated passwords, whereas all 7 participants with stand-alone password managers adopt random passwords.

Nudging. Nudging, a concept in behavioral science, aims to influence decisions without limiting people's choices [23]. Nudging has been employed in many contexts, and is of interest to a broad range of human-computer interaction (HCI) topics [9]. In cybersecurity, it has been used in many security decisions [58], including which Wi-Fi network to join [57], social network posts to make [55], and emails to trust [11]. Nudging has also been applied to tackle the problem of password creation in alphanumerical passwords (through password strength meters [43, 44]) and graphical passwords [37, 51], and password manager adoption [2, 4]. Nudging has also been studied in the context of promoting users to accept randomly-generated passwords [23]; although the studied nudges were unsuccessful, they were quite different than those employed by current password managers.

Our work. Nudging is employed by a number of popular browser's built-in password managers: Chrome, Firefox, and Safari (see Figure 1b-d). However, the efficacy of these nudges has not yet been studied, to the best of our knowledge. In this paper, we study the efficacy of these browser nudges, factors that may influence their efficacy, and users' reasoning for accepting (or not accepting) the nudge. Our goal is to deepen our understanding of what nudges work best in this context, and why, which can be used to help improve the state-of-the-art.

3 Methodology

Our primary goal is to evaluate the effectiveness of nudges employed by the three most popular browsers: Chrome, Firefox, and Safari, in terms of their ability to encourage the use of randomly generated passwords. We review the browser nudges studied in Section 3.1. We created a mock-up of a new e-commerce website for purchasing local produce (Figure 1a) to examine user behavior when creating an account on the website. We collected and analyzed quantitative data composed of users' decisions while creating an account (e.g., if a randomly generated password is adopted) and both quantitative and qualitative data from users' responses to a questionnaire. Our study was reviewed and approved by our institution's Research Ethics Board. We explain the structure of our study further in Section 3.2. Our recruitment method is described in Section 3.5 and resulting demographics are summarized in Section 3.6. We outline our analysis approach in Section 3.7.

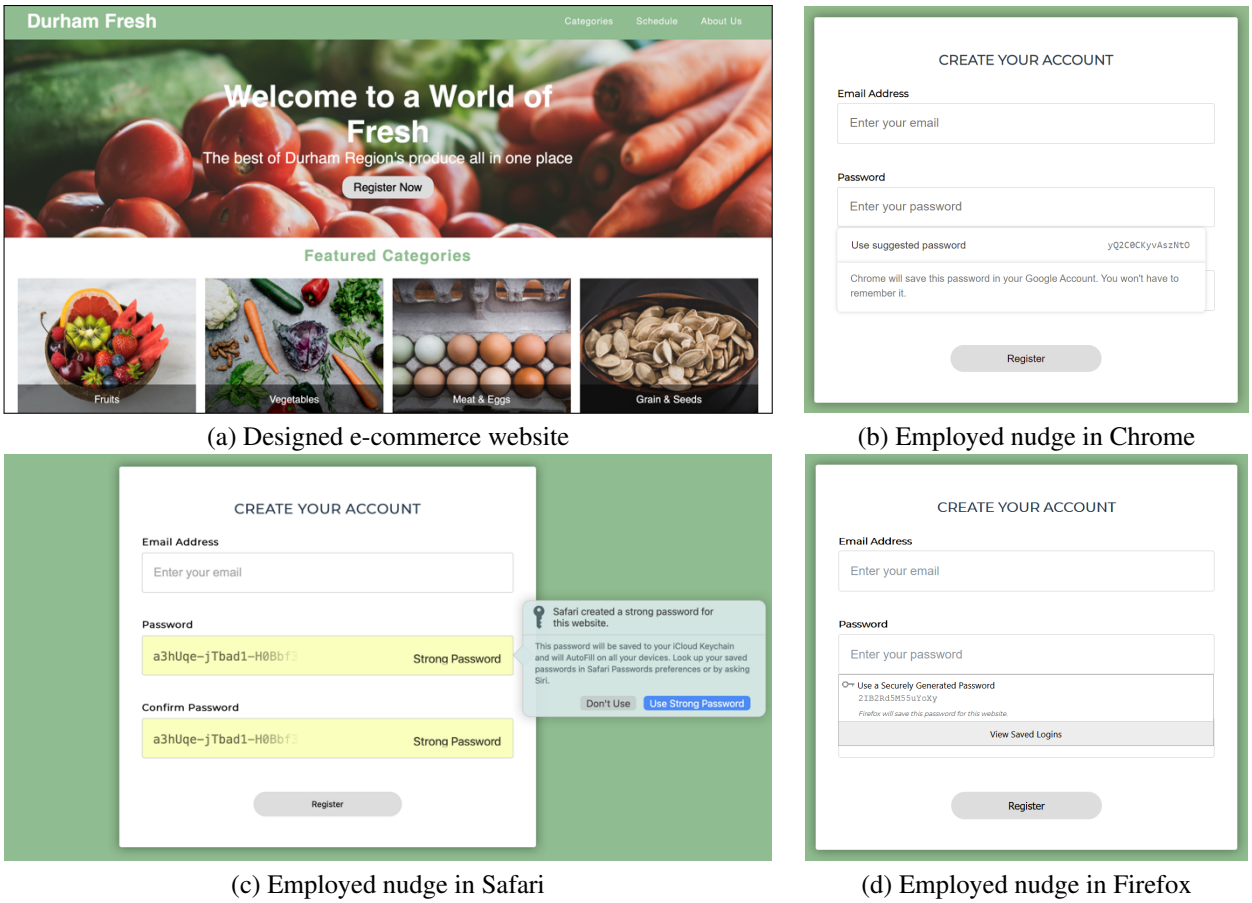
3.1 Nudges in Chrome, Firefox, and Safari

Each browser uses nudges to encourage people to use a random password generator. Chrome's *just-in-time nudge* (see Figure 1b) is displayed when a user clicks the password field. This nudge suggests the user a 15-character randomly generated password to encourage its adoption. Chrome displays the suggested random password with the message of "Use suggested password", and includes the following statement, "Chrome will save this password in your Google Account. You won't have to remember it." The focus of the nudge appears to be more on convenience than on security with an emphasis on remembering passwords for user. Chrome's nudge is simple and does not seek to grab the user's attention. Firefox's nudge (see Figure 1d) is also a just-in-time nudge and very similar to that of Chrome, even in terms of the length of passwords. Firefox uses the term "Securely" in its message of "Use a Securely Generated Password", followed by the statement of "Firefox will save this password for this website." The main difference in word choice is that Firefox's nudge puts emphasis on security as well as convenience.

Safari (Figure 1c) uses a different method of nudging known as a *default nudge*. A default nudge works by selecting the desired option by default. To encourage the selection of a random password, Safari automatically populates the password field with an 18-character random password when the user clicks in it. Safari's nudge is accompanied by a pop-up message of "Safari created a strong password for this website—This password will be saved to your iCloud Keychain and will AutoFill on all your devices. Look up your saved passwords in Safari Password preferences or by asking Siri". Safari's nudge is the most visually diverse and puts emphasis on both password strength and convenience. Safari's use of color and a default nudge is a clear attempt to grab user's attention. Furthermore, Safari's description of its password manager's functionality aims to educate users and persuade them to use it.

3.2 Study Structure

We designed our study to employ deception in order to keep our website registration as realistic as possible, without



(a) Designed e-commerce website

(b) Employed nudge in Chrome

(c) Employed nudge in Safari

(d) Employed nudge in Firefox

Figure 1: Our mock-up website for which study participants were asked to register an account is shown in (a). The browser nudges studied are: (b) Chrome, (c) Safari, and (d) Firefox.

drawing additional attention to the nudge. The users are first falsely informed that the purpose of our study is evaluating the user interface and functionality of our (fake) e-commerce website. However, participants were debriefed with the actual purpose of the study in a secondary consent form and participant data is only collected if they agree to it; otherwise, they were considered to have opted out. For our study, participants were specifically required to do the following tasks:

Task 1: First consent form. Participants were provided with a deceptive consent form that explained the purpose of the study is to help evaluate the usability of our website's registration and login processes (see Appendix A). It did not reveal the study's true focus on passwords and nudging.

Task 2: Account registration. The participants were asked to test the usability of our website's registration and login process by creating an account using a valid email and a password that conforms the password policy. Users have the freedom to create their own passwords or use the browser's password manager for a randomly generated password. Regardless of how users create their passwords, users are given the option to store their passwords using their browser's password manager.

Task 3: Post-registration questionnaire. We asked participants to answer 5 demographic questions including their age, gender, education, their primary area of study or work, and their first language. See Appendix B for full details.

Task 4: Login. Participants were asked to log in to their accounts created in Task 2 using their email address and chosen passwords. If the users have stored their passwords in the browser's password manager, the password manager would autofill their stored password.

Task 5: Post-study questionnaire. Participants were asked to answer questions focusing on users' behavior relating to the nudges, password managers, and password creation. See Appendix C for full details.

Task 6: Second consent form. Participants were provided with a second (real) consent form (see Appendix D) that explains the true purpose of the study before submission.

3.3 Ethical Considerations

If participants initially knew the purpose of our study, it would bring unrealistic focus to the randomly generated password nudge. Therefore, we used deception by telling participants that they are testing the usability of a new e-commerce

website's registration and login process. Participants were debriefed through a secondary consent form (see Appendix D), which they were asked to read carefully before agreeing to submit their data. Participant data is only stored after they agree to this secondary consent form. To mitigate the risk of users reusing one of their passwords, we only collect/store passwords/data with anonymous identifiers, and only after obtaining secondary consent. Our study was reviewed and approved by our institution's Research Ethics Board.

3.4 Implementation Details

For the account registration task of our study, the password policy for a user is randomly set to be either a 1C8 or 3C12 password policy. A 1C8 policy only requires a minimum of 8 characters, whereas a 3C12 policy requires a minimum of 12 characters with at least 3 character classes of lowercase characters, uppercase characters, special characters, and numbers. We used these two different password policies to analyze users' password decisions when confronted with simple and complex password requirements. Based on the user's browser (Chrome, Firefox, or Safari), our website shows a simulation of the browser's password manager and records their interactions with the simulated password manager. We also ensure the actual password managers are not invoked when the simulated password managers are presented to the user. The simulated password managers are designed to appear identical to the actual password managers, but are intended to facilitate data collection of user's interaction with the password manager. Figure 1b-d are taken from our simulated password managers, which show how carefully they were designed to be identical to the actual password managers.

Our system enforced a number of rules relating to study completion. To improve data quality, users can only have one tab/instance of our study running at a time and are only able to complete our study once. These rules are to prevent biased results from users who have already completed our study. For ethical reasons, we only collect data once users have submitted both consent forms. This means participants who leave the study before providing the final consent will have their data deleted after 10 minutes of inactivity. Once the data is removed from our servers, users will have to restart our study. However, before the 10 minutes is up, users have the option of continuing our study by restoring their closed tab. Between starting the study and seeing the second consent form, a total of 100 participants opted out. To ensure participants' anonymity, we do not collect their emails, we only collect their passwords.

3.5 Recruitment

We tested our study through a pilot study with 5 participants and asked them to provide us with their feedback. We improved our study's design and user interface based on their comments. Our user study was conducted with 561 participants recruited through Amazon's Mechanical Turk (MTurk) website. Participants were limited to those living in the United States. The estimated completion time for this study was about 5 minutes. To be consistent with minimum wage in the United States ($7.25 USD per hour), participants were compensated $0.60 USD for the completion of our study. Participants could choose to sign up for any one of the three MTurk groups, and we used the user-agent header to determine the correct browser is in use.

3.6 Participant Demographics

Table 1 presents an overview of the participant demographics for our study collected through the post-registration questionnaire (see Appendix B). Our participants were composed of 48.4% female, 49.6% male, and 2% who preferred not to specify their gender.

Participants' ages range from 18 to over 50 years old. The majority of participants (39.6%) fell within the 26–35 age group, followed by the age group of 36–50 making up 27.8% of participants. Regarding participants' education level, most participants (54.1%) had a Bachelor's degree, followed by a high school degree (26.3%). The majority of participants in our study (30.1%) belonged to the business and IT field of education or work.

3.7 Analysis

We analyze our results to find whether there are significant differences between the adoption rate of randomly generated passwords for: (1) the three browsers studied, (2) the two implemented password policies (1C8 and 3C12), (3) participants who noticed the nudge vs. those who did not notice the nudge, (4) participants who used a password manager before vs. those who have not, (5) participants who used a random password generator before vs. those who have not, (6) participants who are using their main (daily use) browsers in our study vs. those who did not. We also analyze our results for whether there are significant differences between the rate of saving passwords in the password manager for: (7) the three browsers studied, and (8) participants who noticed the nudge vs. those who did not notice the nudge. Since all of these analyses involve comparing proportions, we use the χ^2 test to find whether there are significant differences between them. Tests were conducted using Bonferroni adjusted alpha levels of 0.006 per test $(0.05/8)$.

We performed a qualitative analysis on the free-form data from our post-study questionnaire, to find underlying reasons participants did (or did not) use randomly generated passwords. We asked our participants, "Can you describe the reason why you used/did not use the random password generator?" Participants' comments were analyzed using an emergent coding approach, and two researchers coded all

		Chrome	Firefox	Safari
Gender	Female	45.5%	41.5%	58.7%
	Male	52.4%	56.9%	39.1%
	N/A	2.1%	1.6%	2.2%
Age	18-25	11.5%	12.8%	27.4%
	26-35	42.4%	38.8%	37.4%
	36-50	25.7%	30.9%	26.8%
	50+	19.4%	16.5%	8.4%
	N/A	1.0%	1.0%	0.0%
Education	High school	23.6%	30.3%	25.1%
	Bachelor's	58.6%	53.7%	49.7%
	Master's	14.1%	9.6%	18.4%
	PhD/higher	1.6%	3.7%	3.4%
	N/A	2.1%	2.7%	3.4%

		Chrome	Firefox	Safari
Study/Work	Social Sci. & Humanities	5.2%	8.5%	6.7%
	Science	6.3%	5.9%	7.8%
	Health Science	7.9%	4.3%	13.4%
	Engineering & Applied Sci.	8.9%	9.6%	4.5%
	Energy & Nuclear Sci.	0.0%	1.1%	1.1%
	Education	8.4%	5.3%	14.5%
	Business & IT	38.2%	30.9%	20.7%
	Other	16.7%	25.4%	24%
	N/A	8.4%	9%	7.3%
Language	English	95.8%	96.8%	88.8%
	French	0.5%	0.0%	0.6%
	Other	2.7%	2.1%	10.6%
	N/A	1.0%	1.1%	1.1%

Table 1: The user demographics across the three browsers

participants' comments independently by categorizing their statements [28]. Some participants described multiple reasons for (not) using randomly generated passwords, and we applied multiple codes to these comments. To measure the reliability of our coding process, we used Cohen's Kappa [28]. Our resulting $\kappa = 0.98$, suggesting near-perfect agreement between the two researchers.

4 Results

We recruited a total of 561 paid users on Amazon MTurk to participate in our study. We removed three responses due to inconsistent answers to an attention check question that asked users to select a specific number from the list (see Question 5 in Appendix C). We examine our research questions using the remaining 558 responses (191, 188, and 179 participants for Chrome, Firefox, and Safari respectively). The difference in group sizes is partly due to the Safari condition taking the longest to fill, whereas Chrome was the fastest.

4.1 Efficacy of Generated Password Nudge

Our results on the effectiveness of the nudges for each built-in password manager are shown in the first row of Table 2. To determine whether any one of these nudges are more effective than others while registering for our website, we test the following hypothesis:

H_0 The randomly generated password adoption rates are similar between the three browser groups.

H_a The randomly generated password adoption rates differ between the three browser groups.

To test this hypothesis, with the browser groups of Chrome, Firefox, and Safari, we used a χ^2 test ($df = 2$, $N = 558$). We reject the null hypothesis H_0 ($\chi^2 = 32.972$, $p < 0.001$) after Bonferroni multiple-test correction. The effect size is moderate (Cramer's $V = 0.24$). Therefore, we accept our alternative hypothesis H_a that the generated password adoption rates differ between the Chrome, Firefox, and Safari browser groups. As shown in Table 2, more users adopted the Safari nudge than the other two browsers. We will discuss possible reasons for Safari's nudge effectiveness in Section 5.1.

	Chrome	Firefox	Safari
RGPs (1C8+3C12)	35.2%	41%	61.5%
RGPs (1C8)	26.5%	34.7%	61.3%
RGPs (3C12)	38.7%	47.3%	61.6%
Saved password	49.2%	55.3%	70.4%

Table 2: Percent of participants who adopted the randomly generated passwords (RGPs), were influenced by the complexity of the website's password policy (1C8 or 3C12), and saved their passwords in a password manager.

4.2 Efficacy of Nudge to Save Passwords

As shown in Table 2, 49.2% of Chrome users, 55.3% of Firefox users, and 70.4% of Safari users saved their passwords in their respective browser-based password manager. All participants who used a random password generator stored them in a password manager, as well as some additional participants who created their own passwords. We analyzed the saved passwords to determine if users were saving their own passwords or randomly generated passwords. 87.3% of the Safari users who saved their passwords saved a randomly generated password. While 74% of Firefox users and 66% of Chrome users saved randomly generated passwords. To determine if any of these nudges are more effective to encourage users to save their passwords, we test this hypothesis:

H_0 The rates of password storage are similar between browser groups.

H_a The rates of password storage differ between browser groups.

Using the χ^2 test ($df = 2$, $N = 558$), we reject the null hypothesis H_0 ($\chi^2 = 15.90$, $p < 0.001$), with weak effect size (Cramer's $V = 0.16$). We conclude that participants did not have similar behavior regarding storing their passwords in a browser-based password manager, and Safari users were more likely to save their passwords.

4.3 Impact of Website's Password Policy

Our results on the effectiveness of the nudges for each built-in password manager under a simple password policy (1C8) and a complex password policy (3C12) are shown in the two middle rows of Table 2. To determine whether the complexity of the website's password policy influences user choice to adopt a generated password, we test the following hypothesis:

H_0 The randomly generated password adoption rates are similar between website password policies.

H_a The randomly generated password adoption rates differ between website password policies.

To test this hypothesis, with the website password policy groups of 1C8 and 3C12, we used a χ^2 test ($df = 1$, $N = 558$). We fail to reject the null hypothesis ($\chi^2 = 3.921$, $p = 0.047$) after Bonferroni correction ($\alpha < 0.006$), so we accept the null hypothesis and suggest that the website's password policy likely does not create enough pressure to impact user's adoption of a generated password.

4.4 Analysis of Possible Adoption Factors

Our goal in this analysis is to understand whether some factors may contribute to user's adoption of generated passwords and the password manager to save passwords. Our post-study questionnaire features several questions related to participants' familiarity with random password generators and password managers. We also ask participants if they noticed the nudges while registering and their reason for using/not using a random password generator.

More specifically, we investigate the following factors to determine their impact on adopting a randomly generated password: (i) noticing the browser's generated password nudge, (ii) experience with using a password manager, (iii) experience with using a random password generator, and (iv) being a regular (daily) user of the browser, since repeated exposure to the nudge may make it easier to ignore. We also investigate (v) whether noticing the browser's nudge could be a factor in users saving their password in the password manager. Table 3 shows the overall frequencies of participants' responses to the post-study questionnaire questions on factors (i)-(iii). Data related to factor (iv) is shown in Table 4. In the following subsections, we test whether each of these factors were related to the adoption of generated passwords in our study. Our analysis suggests that noticing the nudge has an impact on both adopting the randomly generated password and on saving it. Our analysis also suggests that previous use of a password generator impacts users' adoption of randomly generated passwords. However, previous use of a password manager does not influence users' adoption of randomly generated passwords. We found that being a regular (daily) user does not significantly impact the rate of adopting the randomly generated password.

	Chrome	**Firefox**	**Safari**
Used password manager before	68.6%	64.4%	65.9%
Used password generator before	48.2%	53.2%	57.5%
Noticed the nudge	70.2%	71.8%	88.8%

Table 3: Frequencies of participant characteristics based on post-questionnaire data.

	Chrome	**Firefox**	**Safari**
Daily	89%	70.2%	57%
Weekly	6.3%	9.6%	11.2%
Monthly	0.5%	4.8%	9.5%
A few times per year	0.5%	11.2%	16.2%
Never used	3.1%	3.2%	4.5%

Table 4: Frequencies of participant's usage of the browser used in our study (from post-questionnaire data).

4.4.1 Noticing the Nudge on Generated Password

To determine whether participants noticed the nudge, we asked them "Did you notice the recommendation to use a random password while registering on our website?" in our post-study questionnaire (see Question 4 in Appendix C). We investigate their answers to find if there is a significant difference between participants who noticed the nudge and those who did not regarding using random password generators. Table 3 shows that Safari's nudge was most successful at being noticed by participants. We also found that 43.3%, 50.4%, and 59.7% of Chrome, Firefox, and Safari participants who noticed the presence of the nudges used a random password generator in our study. Overall, almost half (48.4%) of the total number of participants who noticed the nudges in our study decided to create their own passwords, regardless of the nudges' urge to use a randomly generated password. Although noticing the nudge increases the acceptance rate of randomly generated passwords, in Safari the acceptance rate decreases slightly (approx. 1%). However, note that only a small number of Safari users (19/179) didn't notice the nudge.

To determine whether noticing the nudge to use a random password influences user choice to adopt a generated password, we test the following hypothesis:

H_0 The randomly generated password adoption rates are similar between participants who noticed vs. did not notice the nudge.

H_a The randomly generated password adoption rates differ between participants who noticed vs. did not notice the nudge.

To test this hypothesis, we used a χ^2 test ($df = 1, N = 558$). Our finding indicates a significant difference between above-mentioned groups of participants in terms of using a random password generator ($\chi^2 = 39.265$, $p < 0.001$). The effect size is moderate (Cramer's $V = 0.26$).

4.4.2 Previous Password Manager and Generator Use

Based on our findings, 53.3%, 53%, and 67% of Chrome, Firefox, and Safari participants who have experience with using password generators before used a random password generator in our study. Accordingly, in terms of having experience with using password managers, 38.2%, 43%, and 64.4% of Chrome, Firefox, and Safari users used a random password generator in our study. To determine whether using a password generator before influences user choice to adopt a generated password, we test the following hypothesis:

H_0 The randomly generated password adoption rates are similar between the participants who have used vs. have not used password generators before.

H_a The randomly generated password adoption rates differ between the participants who have used vs. have not used password generators before.

Additionally, to determine whether using password managers before influences user choice to adopt a generated password, we test the following hypothesis:

H_0 The randomly generated password adoption rates are distributed similarly between participants who have used vs. have not used password managers before.

H_a The randomly generated password adoption rates are distributed differently between participants who have used vs. have not used password managers before.

To test this hypothesis, we used a χ^2 test ($df = 1, N = 558$). Based on our results, participants who were familiar with the password generator are more likely to use it while creating an account ($\chi^2 = 43.842$, $p < 0.001$). The effect size is moderate (Cramer's $V = 0.28$). However, there is no significant difference between users who used a password manager before our study in terms of using a random password generator ($\chi^2 = 5.154$, $p = 0.023$).

4.4.3 Regular Use of Browser

We define a user's *regularly-used browser* as a browser used on a daily basis. If a participant regularly uses a browser, it is possible that they are used to the nudge, and it may be less effective for them. To evaluate whether this might be a factor, we asked participants how often they use the browser they used for our study. Table 4 indicates the percentage of how often the browser was used in each browser group (Chrome, Firefox, and Safari). Further analysis of our data indicated that 42.4% of participants who use Firefox daily used a random password generator in our study. While 68% of participants who use Safari daily used a random password generator. The percentage of daily Chrome users who used a random password generator in our study is 29.4%. Overall, 72.6% of participants in our study indicated that the browser they used for this study is one they use daily. Only 3.6% of participants stated they had no experience using the browser they used to complete our study. Among all participants who were using a regularly used browser to complete our study, 43.5% of them generated their password using a random password generator, which means that more than half of the participants do not adopt the randomly generated password when they are using a regularly used browser. To determine whether using a regularly used browser influences user choice to adopt a generated password, we test the following hypothesis:

H_0 The generated password adoption rates are similar between the participants who used a regularly-used browser vs. the participants who used an infrequently-used browser.

H_a The generated password adoption rates differ between the participants who used a regularly-used browser vs. the participants who used an infrequently-used browser.

To test this hypothesis, we used a χ^2 test ($df = 1, N = 558$). Based on the results ($\chi^2 = 0.81$, $p = 0.366$) there is not a significant difference between these two groups regarding using a random password generator in our study.

4.4.4 Noticing the Nudge on Password Storage

Since storing a password in a password manager is the second primary function of the password manager, we investigate our result to find whether noticing the recommendation to use a random password affects the user's decision to store their password in a browser's password manager. To determine whether noticing the nudge influences user choice to save a password in a browser-based password manager, we test the following hypothesis

H_0 The rates of password storage are similar between the participants who noticed vs. did not notice the nudge.

H_a The rates of password storage differ between the participants who noticed vs. did not notice the nudge.

To test this hypothesis, we used a χ^2 test ($df = 1, N = 558$). Interestingly, participants who saved their passwords in a password manager mostly belong to the group of participants who

noticed the nudge, and the difference between participants who noticed the nudge and then saved their passwords and participants who did not notice the nudge and saved their password in a password manager is remarkable ($\chi^2 = 33.321$, $p < 0.001$). The effect size is moderate (Cramer's $V = 0.24$).

4.5 Why (not) Random Passwords?

The codebook with the frequencies, along with examples for each code is provided in Table 5. When analyzing participants' reasons for using a random password generator, 19.89% of participants from this group reported convenience vs. 12.19% for security. The next most common response was password storage feature (5.56%), meaning random password generators' main appeal is convenience and security. When analyzing participants' reasons for not using a random password generator, 23.66% of participants in this group reported random passwords are too hard to remember. The next most common response was participants preferred to create their own passwords (11.47%), which indicates that the endowment effect may also be a major reason for rejecting randomly generated passwords. It is possible that this reluctance to use randomly generated passwords is rooted in participants feeling unsafe when they are unable to memorize their passwords. Our study confirms others' findings that the main reasons for adopting randomly generated passwords are convenience [39, 45], and security [45], but differs regarding the save password feature's importance [31]. Moreover, Our study confirms other's findings that the main reasons for rejecting randomly generated passwords are memorability issues and user preferences [31, 45], but differs regarding the importance of a lack of awareness [39, 45], trust [45], or concern [39]. We discuss the implications of these findings in Section 5.

5 Discussion

Our study empirically tests the effects of nudges employed by the three most popular browsers: Chrome, Firefox, and Safari. We were also interested in understanding the factors that influence users' decisions while creating a password. The results from our server logs and questionnaires suggest that the majority of the participants from each browser group completed our study using a browser they use regularly, and that regular use of the browser didn't influence adoption of the randomly generated password.

5.1 Possible Reasons for Safari's Effectiveness

Safari had the most effective password manager nudge in terms of influencing participants to use a random password generator and save their passwords. Additionally, our results indicate that Safari has the most noticeable nudge when compared to Chrome and Firefox. Safari's nudge (Figure 1c) is clearly more visually striking than Chrome's or Firefox's nudge. Safari's use of color, an additional pop-up box, and automatically populating the password field with a randomly generated password makes their nudge much more prominent. Chrome and Firefox take a subtle approach to suggest that people use randomly generated passwords. In contrast, Safari's pop-up message includes some information on the storage and autofill features. This is useful for users who are unfamiliar with password managers and may help people become more comfortable adopting this feature. Additionally, Safari uses a default nudge which takes the liberty of populating the password field with a randomly generated password and emphasizes its strength with the message, "Strong password". A quantitative review of 100 publications on nudging which aimed to determine the effectiveness of various nudging techniques states that, "default nudges are the most effective" [17].The effectiveness of default nudges is also shown in two other studies [19, 30]. Therefore, a reason Safari is effective at convincing people to use random passwords could be attributed to the fact that Safari decides for you. Unless users take the effort to create a password themselves, simply using the password provided is more convenient. Alternatively, Safari making the choice to input a random password by default may convince users that it is the recommended action. Safari's nudge clearly expresses that the generated password is strong, implying to the user that it is the optimal password to use. Another interesting element of Safari's design is that it contains a visual effect on the last six characters of the password, giving the impression that the password contains even more characters than are seen. It is possible that this visual effect is interpreted by the user as the password offering even more security, as it appears longer and as though there are parts that couldn't be observed through shoulder-surfing.

In general, we found higher rates of randomly generated password adoption and awareness than another study [39], which found that 14% of Safari users used randomly generated passwords, while Chrome users were unaware of randomly generated passwords. Our results found higher Safari user adoption rates (61%) and also Chrome user awareness of randomly generated passwords (30% adopted randomly generated passwords); this may be due to changes in user behavior over time (2018-2022), or differences in methodology, as their study [39] was conducted through semi-structured interviews ($n = 30$).

5.2 Reasons Participants Used Password Manager Features (or Not)

Our post-study questionnaire (Appendix C) asked participants to specify their reasons for using (or not using) a random password generator. Emergent coding was then used to analyze the free-form, self-reported data from our questionnaire and categorize participants' comments. By categorizing

	Code	Frequency		Examples of participants' reasons on why they used/not used password generator
Reasons for using a random password generator	**Convenience**	111	19.89%	"It seemed convenient to use a securely generated password." "I used it because it seemed faster than creating a new password."
	Security	68	12.19%	"I figured the random password was strong enough so I accepted it." "Random passwords seem more secure, since they cannot be guessed by intruders."
	Remember Password Feature	31	5.56%	"I did because it was saved to Chrome and I can go back in and edit it later if I want." "I used it because it saves my password for the next time I would login to the site."
	Didn't care about the website	26	4.66%	"I selected the random password generator because it is a tempt site." "I didn't want to think of an actual password for this site."
	Avoid reusing passwords	23	4.12%	"I did not want to use one of my regular passwords. "I rather not give a random site a password I would usually use."
	Noise	9	1.61%	"NONE" "I did use it."
	Strict password policy	9	1.61%	"I used it because I couldn't really think of a 12 character password." "I did use it. I used it because it tried to require a 12 digit password, and that is too long to make up myself."
	Preferred to use a generator	7	1.25%	"I used the generator because I usually always do." "Habit. I've always generated/used single use passwords per website/service."
	Incongruous	5	0.90%	"If the password manager were to fail I would lose all my passwords." "I wanted to create my password from scratch and not use anything else."
	Unsure	5	0.90%	"I am confused and not aware of this option." "I was not looking for it!"
Reasons for self-chosen password	**Memorability issue**	132	23.66%	"Random is hard to remember if you need to login on another device." "I did not use the random password generator because I am afraid I will forget it!"
	Prefer to create their own passwords	64	11.47%	"I would prefer using a word i am more familier with than any suggestions." "I'd rather use a unique password that I create."
	Didn't notice the nudge	24	4.30%	"I didn't realize I could." "Didn't notice the option."
	Trust issue	23	4.12%	"I don't believe in random password generator. May be the website hacks my details. So I'll be careful in this." "I don't trust that technology. I'd rather create my own password and then write it down."
	Noise	20	3.58%	"None" "My pet name"
	Security concerns	16	2.87%	"I don't feel safe using a generator that I have not used before." "Because it wasn't strong enough."
	Didn't care about the website	13	2.33%	"I didn't use it because I'm not going to be using this site again." "Because i do not plan to use this site so it's not relevant"
	Incongruous	13	2.33%	"I used the password manager because there are too many things sites that I use that need different passwords and I couldn't remember all of them." "I used it because its the safest way to create a password."
	The desire to reuse password	9	1.61%	"Because I usually keep one password to all. . . " "I just prefer to use the same password for stuff so that it is easier to remember."
	Lack of knowledge of password manager	3	0.54%	"I didn't know how to use it."

Table 5: Codebook: Reasons for adopting/not adopting a randomly generated password. As multiple codes were assigned to several comments, the summation of frequencies for each reason is more than the number of participants.

participants' comments, we could spot trends in user behavior. For instance, convenience and security were the most common reason participants adopted the randomly generated password, while memorability issues were participants' main reason for not using a random password generator. The purpose of random password generators is to provide a convenient method for creating secure passwords, which coincides with participants' reasons for using them. However, random passwords are complex and difficult to remember to prevent brute-force and guessing attacks [54]. Since random passwords are hard to remember, password generators are accompanied by password managers, which store the generated passwords. If password managers solve the issue of random password memorability, why do people reject using them? Based on participants' comments from our post-study questionnaire, people prefer to remember their passwords in order to use them on different devices. One participant commented, "Random [password] is hard to remember if you need to login on another device." Browser-based and third-party password managers sync passwords across devices, ensuring users always have access to their passwords. Safari's nudge includes the message, "Safari created a strong password for this website—This password will be saved to your iCloud Keychain and will AutoFill on all your devices." This message informs users that they will have access to their passwords across devices that use iCloud Keychain. Chrome and Firefox, however, do not have messages explicitly stating that users will have access to their passwords across devices, which may be why people are hesitant to save their passwords. Participants' comments also expressed a distrust of password managers due to a lack of knowledge of the technology, which corroborates Fagan et al.'s study [12]. Safari was the most effective pass-

word manager likely because it explains the feature to remove doubt from users. Chrome and Firefox's convenient, minimalist approach to nudging lacks a detailed explanation of their password manager's features, leaving unanswered questions in people's minds. A solution to the low adoption of password managers could be to improve their design by adding a more thorough explanation of their features. Doing so might educate users about the benefits of the technology, help build trust with users, and ultimately improve the adoption of password managers.

5.3 Limitations

Our study is categorized as a quasi-experiment because participants were not randomly assigned to each browser, but could sign up for one of the three groups. Thus, it is possible that participants' behavior may be due to differences between Chrome, Firefox, and Safari users, rather than the differences between browser nudges. However, randomly assigning participants to each group posed its own issues: if participants were assigned to an unfamiliar browser, they may be more likely to (a) drop out since it is not installed or (b) notice the nudge more often since they aren't familiar with the browser. These issues would affect users' behavior and therefore the accuracy of our results. We also considered emulating each browser's nudge on a single browser (e.g., Chrome); however, users who are familiar with the browser may notice the change in the browser's nudge design, suspect our intentions, and alter their behavior accordingly. Therefore, we decided on a quasi-experiment design for this study.

There are some limitations from running our study on Amazon MTurk. First, our study had limited diversity because participants were all Amazon Mechanical Turk workers from the United States. MTurk workers are younger and more tech-savvy than the average population [42]. However, previous research implies that online privacy and security behavior studies can estimate the general population's behavior despite this flaw [42]. Second, the Amazon MTurk platform's prevalence of poor data quality has been increasing [26]. As a result, we used various countermeasures, such as validating participants' MTurk IDs and putting a verification question to catch invalid study attempts. These countermeasures excluded invalid data from further analysis and prevented participants from taking our study more than once. However, it is possible that the nature of the study (single session/one device, no requirement to return) encouraged the use of the password manager more than longer-term scenarios. Also, it is possible that MTurk workers may encounter more account creation scenarios than most, leading to a higher adoption rate of randomly generated passwords.

Having the questionnaires and consent forms in English required participants to be fluent in English, and may have resulted in a language or cultural bias. Regarding questionnaire responses, like any self-reported data, they may be vulnerable to a social desirability bias [13] and may differ from natural behavior due to privacy paradox [27]. To ensure participants answer honestly, the true intent of the study is not revealed until all tests and questionnaires have been completed. Initially, participants are told they are testing the registration system for a new website and are unaware of our goal to test the effectiveness of browser nudges. This allows us to test how participants would naturally create a new account for a website and helps eliminate social desirability bias.

Some users in our study may have been making use of other password managers and/or random password generators. We analyzed participants' passwords to determine if third-party software may have been used to generate passwords as an alternative to browsers' built-in password generators. For this purpose, we check whether users typed or pasted their password in a password field. According to our data, 7.9% of Chrome participants, 4.8% of Firefox participants, and 1.7% of Safari participants used alternative methods to generate passwords and paste them into the password field while registering.

6 Conclusion

We conducted a user study on the nudges employed by the built-in password managers in Chrome, Firefox, and Safari by using a mock e-commerce website. We investigated the effectiveness of the nudges in terms of their ability to encourage users to adopt a randomly generated password while registering. Moreover, we investigated whether a number of factors influence users' toward adopting a randomly generated password. Our findings indicate that Safari works better in terms of its ability to encourage people to use a random password generator. Notably, participants in the Safari group believed that the nudge employed by Safari is more noticeable. Some reasons for Safari's nudge being more noticeable are that (a) Safari is using a default nudge, which automatically populates the password field with a suggested password, (b) it uses color and a pop-up message, and (c) it implements interesting visual effects on the randomly generated password. We were surprised to find that implementing a strict password policy does not seem to influence participants to use a random password generator. Although one would assume selecting a random password is easier than creating a password that conforms to a 3C12 password policy, it would appear many people are still more comfortable creating their own passwords. Our results show that "default nudges" also work well for password managers, which is consistent with other studies suggesting that default nudges are the most effective nudge type across many fields [17, 19, 30].

Future work includes dissecting the reasons for Safari's nudge performing better, to identify exactly which design elements are most impactful. This could be done by trying different variations of the nudge, where each implements only one of the design elements. It is possible that the default

aspect of the nudge is most important, or alternatively it could be due to the prominence of the nudge. While one of our findings was that users who noticed the nudge were more likely to accept a randomly generated password, future studies involving more prominent nudges should be aware of potential risks such as habituation. Additionally, some research suggests that personalizing nudges to match a user's decision-making behavior results in more impactful nudges [34]. However, implementing personalized nudges is a challenging endeavor that requires several phases [40]. This may be an interesting avenue for future work in password manager nudges. Since this study was conducted on Amazon Mturk, long-term studies with a non-crowdsourced population are needed. Also, the effectiveness of other forms of nudging [9, 17] for adoption of randomly generated passwords could be explored.

References

[1] Rowe Adam. Study reveals average person has 100 passwords. https://tech.co/password-managers/how-many-passwords-average-person. Accessed: 2022-06-03.

[2] Yusuf Albayram, John Liu, and Stivi Cangonj. Comparing the effectiveness of text-based and video-based delivery in motivating users to adopt a password manager. In *European Symposium on Usable Security 2021*, pages 89–104, 2021.

[3] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? In *European Workshop on Usable Security*, 2016.

[4] Nora Alkaldi and Karen Renaud. Encouraging password manager adoption by meeting adopter self-determination needs. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[5] Fahad Alodhyani, George Theodorakopoulos, and Philipp Reinecke. Password managers—it's all about trust and transparency. *Future Internet*, 12:189, 2020.

[6] Sal Aurigemma, Thomas Mattson, and Lori Leonard. So much promise, so little use: What is stopping home end-users from using password manager applications? In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[7] Jannatul Bake Billa, Anika Nawar, Md Maruf Hasan Shakil, and Amit Kumar Das. Passman: A new approach of password generation and management without storing. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, pages 1–5. IEEE, 2019.

[8] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (S&P)*, pages 553–567, 2012.

[9] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2019.

[10] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, volume 15, pages 1–16, 2006.

[11] Molly Cooper, Yair Levy, Ling Wang, and Laurie Dringus. Subject matter experts' feedback on a prototype development of an audio, visual, and haptic phishing email alert system. *Online Journal of Applied Knowledge Management*, 8(2):107–121, 2020.

[12] Michael Fagan, Yusuf Albayram, Mohammad Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 2017.

[13] Robert J. Fisher. Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research*, 20(2):303–315, 1993.

[14] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657–666, 2007.

[15] Shirley Gaw and Edward W. Felten. Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable privacy and Security*, pages 44–55, 2006.

[16] David Halpern. *Inside the nudge unit: How small changes can make a big difference*. Random House, 2015.

[17] Dennis Hummel and Alexander Maedche. How effective is nudging? a quantitative review on the effect sizes and limits of empirical nudging studies. *Journal of Behavioral and Experimental Economics*, 80, 2019.

[18] Troy Hunt. Have i been pwned: Check if your email has been compromised in a data breach. https://haveibeenpwned.com/. Accessed: 2022-02-16.

[19] Moritz Ingendahl, Dennis Hummel, Alexander Maedche, and Tobias Vogel. Who can be nudged? examining nudging effectiveness in the context of need for cognition and need for uniqueness. *Journal of Consumer Behaviour*, 20(2):324–336, 2021.

[20] Iulia Ion, Rob Reeder, and Sunny Consolvo. No one can hack my mind: Comparing expert and non-expert security practices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 327–346, 2015.

[21] Blake Ives, Kenneth R. Walsh, and Helmut Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.

[22] Shouling Ji, Shukun Yang, Anupam Das, Xin Hu, and Raheem Beyah. Password correlation: Quantification, evaluation and application. In *Proceedings of the IEEE Conference on Computer Communications*, pages 1–9, 2017.

[23] Shipi Kankane, Carlina DiRusso, and Christen Buckley. Can we nudge users toward better password management? an initial study. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

[24] Ambarish Karole, Nitesh Saxena, and Nicolas Christin. A comparative usability evaluation of traditional password managers. In *Proceedings of the 13th International Conference on Information Security and Cryptology*, 2010.

[25] Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and L Julio. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (S&P)*, pages 523–537, 2012.

[26] Ryan Kennedy, Scott Clifford, Tyler Burleigh, Philip D. Waggoner, Ryan Jewell, and Nicholas J. G. Winter. The shape of and solutions to the mturk quality crisis. *Political Science Research and Methods*, 8(4):614–629, 2020.

[27] Spyros Kokolakis. Privacy attitudes and privacy behaviour. *Computer Security*, 64:122–134, 2017.

[28] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Morgan Kaufmann, 2017.

[29] Thomas C. Leonard, Richard H. Thaler, and Cass R. Sunstein. Nudge: Improving decisions about health, wealth, and happiness, 2008.

[30] Yiling Lin, Magda Osman, and Richard Ashcroft. Nudge: concept, effectiveness, and ethics. *Basic and Applied Social Psychology*, 39(6):293–306, 2017.

[31] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. Better managed than memorized? studying the impact of managers on password strength and reuse. In *Proceedings of the 27th USENIX Conference on Security Symposium)*, pages 203–220, 2018.

[32] William Melicher, Blase Ur, Sean M. Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Fast, lean, and accurate: Modeling password guessability using neural networks. In *Proceedings of the 25th USENIX Security Symposium*, pages 175–191, 2016.

[33] Burak Merdenyan and Helen Petrie. Perceptions of risk, benefits and likelihood of undertaking password management behaviours: Four components. In *Human-Computer Interaction – INTERACT 2019*, pages 549–563. Springer International Publishing, 2019.

[34] Stuart Mills. Personalized nudging. *Behavioural Public Policy*, 6(1):150–159, 2022.

[35] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond credential stuffing: Password similarity models using neural networks. In *IEEE Symposium on Security and Privacy*, pages 417–434, 2019.

[36] Zach Parish, Connor Cushing, Shourya Aggarwal, Amirali Salehi-Abari, and Julie Thorpe. Password guessers under a microscope: An in-depth analysis to inform deployments. *International Journal of Information Security*, 2021.

[37] Zach Parish, Amirali Salehi-Abari, and Julie Thorpe. A study on priming methods for graphical passwords. *Journal of Information Security and Applications*, 62:102913, 2021.

[38] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310, 2017.

[39] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, 2019.

[40] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior*, 109:106347, 2020.

[41] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *Proceedings of the 30th USENIX Security Symposium*, 2021.

[42] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1326–1343, 2019.

[43] Karen Renaud, Verena Zimmerman, Joseph Maguire, and Steve Draper. Lessons learned from evaluating eight password nudges in the wild. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*, pages 25–37, 2017.

[44] Karen Renaud and Verena Zimmermann. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, 3(2):228–258, 2018.

[45] Sunyoung Seiler-Hwang, Patricia Arias-Cabarcos, Andrés Marín, Florina Almenares, Daniel Díaz-Sánchez, and Christian Becker. "i don't see why i would ever want to use it" analyzing the usability of popular smartphone password managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1937–1953, 2019.

[46] James Simmons, Oumar Diallo, Sean Oesch, and Scott Ruoti. Systematization of password manageruse cases and design paradigms. In *Annual Computer Security Applications Conference*, pages 528–540, 2021.

[47] Elizabeth Stobert and Robert Biddle. A password manager that doesn't remember passwords. In *Proceedings of the 2014 New Security Paradigms Workshop*, pages 39–52, 2014.

[48] Elizabeth Stobert and Robert Biddle. The password life cycle. *ACM Transactions on Privacy and Security*, 21(3), 2018.

[49] Elizabeth Stobert, Tina Safaie, Heather Molyneaux, Mohammad Mannan, and Amr Youssef. Bypass: Reconsidering the usability of password managers. In *International Conference on Security and Privacy in Communication Systems*, pages 446–466. Springer, 2020.

[50] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, et al. Protecting accounts from credential stuffing with password breach alerting. In *28th USENIX Security Symposium (USENIX Security '19)*, pages 1556–1571, 2019.

[51] Julie Thorpe, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. The presentation effect on graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2947–2950, 2014.

[52] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. I added '!' at the end to make it secure: Observing password creation in the lab. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 123–140, 2015.

[53] Rafael Veras, Christopher Collins, and Julie Thorpe. A large-scale analysis of the semantic password model and linguistic patterns in passwords. *ACM Transactions on Privacy and Security*, 24(3), 2021.

[54] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. Targeted online password guessing: An underestimated threat. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1242–1254, 2016.

[55] Yang Wang, Pedro Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Cranor. Privacy nudges for social media: an exploratory facebook study. In *Proceedings of the 22nd International Conference on World Wide Web*, 2013.

[56] Shannon Williams. Average person has 100 passwords - study. https://securitybrief.co.nz/story/average-person-has-100-passwords-study. Accessed: 2022-02-17.

[57] Iryna Yevseyeva, Charles Morisset, and Aad van Moorsel. Modeling and analysis of influence power for information security decisions. *Performance Evaluation*, 98:36–51, 2016.

[58] Verena Zimmermann and Karen Renaud. The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction*, 28(1), 2021.

Appendix A First Consent Form

Title of Research Study: Evaluating the Usability of the Registration/Login Process of an E-Commerce Website.

Introduction: You are invited to participate in a research study entitled Evaluating the Usability of the Registration/Login Process of an E-Commerce Website. Please read the information about the study presented in this form. The form describes the study's procedures, risks and benefits that you should know before you decide if you would like to take part. You should take as much time as you need to make your decision. You should ask the Principal Investigator (PI) or study team to explain anything that you do not understand and make sure that all of your questions have been answered before signing this consent form. Before you make your decision, feel free to talk about this study with anyone you wish including your friends and family. Participation in this study is voluntary. This study has been reviewed by the University of Ontario Institute of Technology (Ontario Tech University) Research Ethics Board 16544 on October 17, 2021.

Purpose: You have been invited to participate in this study because your participation can contribute to our evaluation of the usability of the registration/login process for our website.

Procedure: This study will take about 5 minutes, and you will be provided with $0.60 USD upon completion of our study and survey. The study tasks include:

- You will be taken to the Registration page of our website and asked to register.
- We will ask you some demographic questions.
- You will be taken to the Login page of our website and asked to login.
- We will ask you some additional questions and to provide feedback.

Potential Benefits: You will be compensated with $0.60 USD for participation and completion of your task and survey.

Potential Risk or Discomforts: There are no known or anticipated risks to you from participating in this study.

Use and Storage of Data: The data includes demographic information and feedback (i.e., gender, age, and education level). All the data is anonymous and the data doesn't include any personal, confidential, or valuable information.

Confidentiality: Your MTurk ID will be kept confidential. Collected data will be anonymous and it will not include any information that reveals your identity. Please note that to maintain your registration experience on our website, you will be asked to enter an email address, but this information will not be stored. Your privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data is in transit over the Internet. This research study includes the collection of demographic data which will be aggregated in an effort to protect your anonymity. Despite best efforts it is possible that your identity can be determined even when data is aggregated.

Voluntary Participation: Your participation in this study is voluntary. You may also decide not to be in this study. or to leave the study at any time. You will be given information that is relevant to your decision to continue or withdraw from participation. You may refuse to answer any question you do not want to answer.

Right to Withdraw: If you withdraw from the research project prior to your final submission and the end of the study tasks, any data will be removed from the study and you do not need to offer any reason for making this request. You can withdraw within one week of submitting your data by contacting the researchers directly by email.

Compensation, Reimbursement, Incentives: You will be compensated with $0.60 USD for participation and completion of your task and survey. You won't be compensated if you do not submit your data at the end of the study.

Debriefing and Dissemination of Results: If you are interested in learning of the results, please contact Samira Zibaei at Samira.Zibaei@ontariotechu.net.

Participant Rights and Concerns: Please read this consent form carefully and feel free to ask the researcher any questions that you might have about the study. If you have any questions about your rights as a participant in this study, complaints, or adverse events, please contact the Research Ethics Office at (905) 721-8668 ext. 3693 or at researchethics@ontariotechu.ca. If you have any questions concerning the research study or experience any discomfort related to the study, please contact the researcher Samira Zibaei at Samira.Zibaei@ontariotechu.net.

Secondary Use of Research for Future Research Purposes: Please note, if you agree to participate (and do not withdraw from the study), your anonymous data may also be used for future studies relating to our research.

Consent to Participate:

1. I have read the consent form and understand the study being described.
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future.
3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty.
4. I understand the possible need for secondary research uses of my research data for future research use and provide consent for the use of my data to be used in future studies.

○ I agree

Appendix B Post-Registration Questionnaire

1. What gender do you identify as?
   - ○ Female
   - ○ Male
   - ○ Prefer not to answer

2. What is your age?
   - ○ 18 – 25 years old
   - ○ 26 – 35 years old
   - ○ 36 – 50 years old
   - ○ 50 +
   - ○ Prefer not to answer

3. What is the highest degree or level of education you have completed?
   - ○ High school
   - ○ Bachelor's degree
   - ○ Master's degree
   - ○ PhD or higher
   - ○ Prefer not to answer

4. What is your first language (i.e., mother tongue)?
   - ○ English
   - ○ French
   - Other: _____
   - ○ Prefer not to answer

5. What is your primary area of study or work?
   - ○ Social Sciences and Humanities
   - ○ Science
   - ○ Health Science
   - ○ Engineering and Applied Science
   - ○ Energy and Nuclear Science
   - ○ Education
   - ○ Business and IT
   - ○ Prefer not to answer

Appendix C Post-Study Questionnaire

1. How often do you use the browser you used in this study?
   - ○ I use this browser daily
   - ○ I use this browser weekly
   - ○ I use this browser monthly
   - ○ I use this browser a few times per year
   - ○ I have never used this browser before today
   - ○ Prefer not to answer

2. Have you ever used a password manager before registering on our website today?
   - ○ Yes
   - ○ No
   - ○ Prefer not to answer

3. Have you ever used a random password generator before registering on our website today?
   - ○ Yes
   - ○ No
   - ○ Prefer not to answer

4. Did you notice the recommendation to use a random password while registering on our website?
   - ○ Yes
   - ○ No
   - ○ Prefer not to answer

5. Please select "Seven" from the following list.
   - ○ 1
   - ○ 5
   - ○ 7
   - ○ 3

6. Can you describe the reason why you used/did not use the random password generator?
   Answer: _____

7. We are interested in any other comments you might have concerning your experience during registration. Please write any thoughts you'd like to share with us.
   Answer: _____

Appendix D Second Consent Form

Title of Research Study: A Study of Nudging to Encourage Random Password Generation

Introduction: You are participating in this research study, and you were asked to evaluate the registration and login process of our proposed E-commerce website. However, this research is studying whether your web browser encourages use of generated passwords and storing them in your browser's password manager. Participation in this study is voluntary, and if you prefer not to submit at this step, your data is automatically withdrawn.

This study has been reviewed by the University of Ontario Institute of Technology (Ontario Tech University) Research Ethics Board 16544 on October 17, 2021.

Purpose: The actual purpose of this study is to test the efficacy of web browser nudges, which try to encourage you as a user to use a random password generator while you register on a new website. Using a randomly generated password and storing it in a password manager is considered a more secure strategy than reusing passwords (even partially) across accounts. Be aware that this strategy is recommended for many web accounts (e.g., e-commerce sites), but not for sensitive accounts (e.g., banking and email). For more information about password managers, please see: https://cyber.gc.ca/en/guidance/password-managers-security-itsap30025.

Potential Benefits: You will be compensated with $0.60 USD for participation and completion of your task and survey. By reading the above information, you may have learned about how to improve your password security by using password generators and password managers.

Potential Risk or Discomforts: There are no known or anticipated risks to you from participating in this study.

Use and Storage of Data: The data includes whether you used the random password generator or not, the password you entered, demographic information, and feedback (i.e., gender, age, and education level). All the data is anonymous and the data doesn't include any personal, confidential, or valuable information. Data will be anonymous and your e-mail address will not be saved in our database.

Confidentiality: Your MTurk ID will be kept confidential and deleted upon completion of the study. Collected data will be anonymous and it will not include any information that reveals your identity. Your privacy shall be respected. No information about your identity will be shared or published without your permission, unless required by law. Confidentiality will be provided to the fullest extent possible by law, professional practice, and ethical codes of conduct. Please note that confidentiality cannot be guaranteed while data is in transit over the Internet. This research study includes the collection of demographic data which will be aggregated in an effort to protect your anonymity. Despite best efforts it is possible that your identity can be determined even when data is aggregated.

Voluntary Participation: Your participation in this study is voluntary. You may choose to submit your information next in order to complete the study, or withdraw by simply exiting the session.

Right to Withdraw: You may withdraw from the research project by not submitting your data next. Also for the next week, you can still withdraw by contacting the researchers by email. Any data will be removed from the study and you do not need to offer any reason for making this request.

Compensation, Reimbursement, Incentives: You will be compensated with $0.60 USD for participation and completion of your task and survey. You won't be compensated if you do not submit next and your collected data will be deleted permanently from our database.

Debriefing and Dissemination of Results: If you are interested in learning of the results, please contact Samira Zibaei at Samira.Zibaei@ontariotechu.net.

Participant Rights and Concerns: Please read this consent form carefully and feel free to ask the researcher any questions that you might have about the study. If you have any questions about your rights as a participant in this study, complaints, or adverse events, please contact the Research Ethics Office at (905) 721-8668 ext. 3693 or at researchethics@ontariotechu.ca. If you have any questions concerning the research study or experience any discomfort related to the study, please contact the researcher Samira Zibaei at Samira.Zibaei@ontariotechu.net.

Secondary Use of Research for Future Research Purposes: Please note, if you agree to participate (and do not withdraw from the study), your anonymous data may also be used for future studies relating to our research.

Consent to Participate:

1. I have read the consent form and understand the study being described.
2. I have had an opportunity to ask questions and my questions have been answered. I am free to ask questions about the study in the future.
3. I freely consent to participate in the research study, understanding that I may discontinue participation at any time without penalty.
4. I understand the possible need for secondary research uses of my research data for future research use and provide consent for the use of my data to be used in future studies.

○ I agree