# Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory

YIXIN ZOU*, Max Planck Institute for Security and Privacy, Germany

KHUE LE, University of Michigan, USA

PETER MAYER, University of Southern Denmark, Denmark

ALESSANDRO ACQUISTI, Carnegie Mellon University, USA

ADAM J. AVIV, The George Washington University, USA

FLORIAN SCHAUB, University of Michigan, USA

We draw on the Protection Motivation Theory (PMT) to design interventions that encourage users to change breached passwords. Our online experiment ($n$=1,386) compared the effectiveness of a threat appeal (highlighting the negative consequences after passwords were breached) and a coping appeal (providing instructions on changing the breached password) in a 2x2 factorial design. Compared to the control condition, participants receiving the threat appeal were more likely to intend to change their passwords, and participants receiving both appeals were more likely to end up changing their passwords. Participants' password change behaviors are further associated with other factors, such as their security attitudes (SA-6) and time passed since the breach, suggesting that PMT-based interventions are useful but insufficient to fully motivate users to change their passwords. Our study contributes to PMT's application in security research and provides concrete design implications for improving compromised credential notifications.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**; • **Security and privacy → Human and societal aspects of security and privacy**.

Additional Key Words and Phrases: Data Breach, Passwords, Protection Motivation Theory, Threat Appeal, Coping Appeal, Online Experiment.

**ACM Reference Format:**
Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, and Florian Schaub. 2024. Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Trans. Comput.-Hum. Interact.* 1, 1, Article 1 (April 2024), 45 pages. https://doi.org/10.1145/1122445.1122456

## 1 INTRODUCTION

Data breaches are increasing, and they expose users and service providers to significant risks [97]. The types of data compromised range from personal identifiers to health information, bank accounts, emails, and passwords [47]. The website haveibeenpwned.com has documented billions of compromised account credentials due to data breaches, including those involving high-profile service providers such as Yahoo!, LinkedIn, and Dropbox [46]. These stolen credentials often end

---

*Work primarily done when the author was a Ph.D. student/postdoc at the University of Michigan.

Authors' addresses: Yixin Zou, yixin.zou@mpi-sp.org, Max Planck Institute for Security and Privacy, Germany; Khue Le, khuele@umich.edu, University of Michigan, USA; Peter Mayer, mayer@imada.sdu.dk, University of Southern Denmark, Denmark; Alessandro Acquisti, acquisti@andrew.cmu.edu, Carnegie Mellon University, USA; Adam J. Aviv, aaviv@gwu.edu, The George Washington University, USA; Florian Schaub, fschaub@umich.edu, University of Michigan, USA.

---

up on the dark web and become trading assets to cybercriminals [104]. With the stolen credentials, attackers can try to break into online accounts at scale through automated login requests, meaning that the breach of one service provider's password database can put other accounts using the same or similar passwords at risk [118]. Compromised accounts can be used for further malicious activities such as impersonation scams and identity theft [77].

Prior work has examined people's reactions to data breaches [55, 69, 128] and password-related behaviors [20, 34, 119]. Users underestimate the potential harms of data breaches [128], reuse a majority of their passwords across sites [20], and exhibit misconceptions about password security [34, 111]. Only between one-quarter to half of all users end up modifying their passwords following data breaches or upon receiving password reset notifications [34, 45, 105]. The low frequency of password changes, compounded by the severity of password attacks, calls for novel approaches to more effectively encourage users to change their passwords after being affected by a data breach.

In our research, we apply the Protection Motivation Theory (PMT) to achieve this goal. We landed on PMT due to the theory's emphasis on fear appeals and mapping with consumer behaviors in response to data breaches. Past research has provided empirical evidence that consumers' inaction after breaches could be attributed to low threat perceptions [43, 69, 128]. Other work has shed light on coping-related impediments that prevent consumers from taking specific actions, such as financial costs [68, 128] and the action being tiresome and tedious [43].

Drawing on PMT, we explore the design space of more effective breach notifications via an online experiment ($n$=1,386). We assess the effectiveness of PMT-grounded interventions on individuals' password change behavior by measuring participants' self-reported intentions and actions. We randomly assigned participants to one of three treatment conditions — a threat appeal, a coping appeal, or both — in addition to a control condition in which changing the breached password was recommended, but no appeal was included. We ensured the ecological validity of our experiment by situating our interventions in real-world breaches recorded by Have I Been Pwned (HIBP) so that participants were reacting to passwords that had indeed been compromised in data breaches and subjected them to further risks.

We find that compared to the control condition, the threat appeal alone made participants 1.48 times more likely to report the intention to change their passwords; when presented together, the threat and coping appeals made participants 1.54 times more likely to report having changed their passwords. We find no statistically significant difference between the three treatment conditions. Password change intentions and actions are also associated with other covariates related to user characteristics (e.g., security attitudes) and contextual factors (e.g., whether the password is reused and time passed since the breach occurred), suggesting that PMT-based interventions alone are useful but insufficient to motivate users to change their passwords. We further identify numerous challenges participants experienced when trying to change their passwords: some forgot the password, while others could not find an account with the breached site. Taken together, our findings show the promise of PMT-grounded interventions for motivating password change behavior while contributing new perspectives on inaction. Not changing passwords after data breaches could be reasonable when users take alternative actions that still protect them. Moreover, inaction in this case might be inevitable due to fundamental issues with the password ecosystem.

## 2 BACKGROUND AND RELATED WORK

We review related work on the Protection Motivation Theory, which serves as the theoretical foundation for this work. We then review prior literature on password policies, behaviors, and interventions to appropriately contextualize PMT's usage for our study's purpose.

## 2.1 Protection Motivation Theory

*PMT overview.* The Protection Motivation Theory (referred to as "PMT" onward) is a psychological theory that explains how individuals respond to threats through two main cognitive processes: threat appraisal and coping appraisal [85, 86]. The threat appraisal involves considering the negative consequences of the threat if it occurs (*perceived severity*) and one's susceptibility to the threat (*perceived vulnerability*) [85]. The coping appraisal involves evaluating the efficacy of a recommended protective behavior (*response efficacy*) [85], one's confidence in performing the action (*self-efficacy*) [122], and barriers to taking action such as financial costs and time investment (*response costs*) [29].

PMT was originally developed by Rogers [85] in the 1970s, and was revised in the 1980s to include reward and self-efficacy components [65, 86]. PMT has been primarily applied in the health domain to design interventions aimed at encouraging healthy behaviors, such as quitting smoking and exercising [29]. Other work has also applied PMT to motivate pro-environmental behaviors [57] or craft safety messages [33].

PMT is an example of social cognitive models, i.e., models that describe how cognitive factors (such as beliefs and perceptions) determine people's responses to social and environmental cues [CITE]. In this sense, PMT shares connections with other social cognitive theories — such as the Health Belief Model [49], the Theory of Planned Behavior [2], and the Transactional Model of Stress and Coping [63] — which similarly focus on how cognitive evaluations lead to protection behaviors. PMT is also closely related to fear appeals, i.e., messages designed to elicit fear by highlighting the consequences of not taking protective action [124], and PMT provides a theoretical framework for understanding how fear appeals work. Our application of PMT represents the fear appeal case, as we explore the theory's efficacy in informing an intervention for motivating password changes after breaches.

*PMT in security and privacy research.* Previous information security and privacy research has primarily used PMT as a social cognitive model to explain protective behaviors in enterprise settings, such as employees' computer security behaviors and adherence to organizational security policies [11, 18, 42, 48, 75, 96, 125]. Other studies have applied PMT to examine end-users' interactions with data backups [10], home computers [7, 40], smartphone locking [3, 4], passwords [115], mobile payment apps [99] and the Tor browser [100]. In addition to threat and coping appraisals, researchers have highlighted the role of other cognitive factors in influencing security and privacy behaviors; example factors include personal responsibility [9, 59, 94], attitudes [96], social norms [42, 53, 96], psychological capital [11], and prior negative experience [64].

Our focus is applying PMT to develop interventions that promote security behaviors, which has been done less often in prior security and privacy research. Existing intervention studies often compare a PMT condition (combining threat and coping appeals) with a control condition [4, 10, 51, 99, 100], showing that PMT-based interventions promote more secure behaviors consistently across contexts. The result may indicate that increasing protection motivation requires both threat and coping appeals, but to test this hypothesis, we need to also examine the effects of threat and coping appeals in isolation, and prior work has provided relatively limited insights on this. Our research takes inspiration from van Bavel et al.'s study, in which the authors separated threat and coping appeals in examining their effects on four behaviors related to online security; they found that the coping appeal was as effective as both appeals combined, but not so the threat appeal alone [114].

From existing literature, there is no consensus regarding the relative dominance between threat and coping appraisals. While many studies have identified coping appraisal as a significant predictor of security intention or behavior [9, 11, 18, 40, 42, 48, 53, 59, 64, 75, 96], some studies also found significant effects for threat severity and/or vulnerability [7, 11, 42, 48, 53, 64, 96]. Other studies

suggest that threat perceptions did not directly impact intention or behavior, but moderated the effect of coping-related constructs [75] or had interaction effects with the individual's other characteristics [18]. A possible explanation of threat appraisal's limited impact in some cases is that the assumption of the threat being personally relevant to the message recipient does not always hold, especially in enterprise security settings. Threats such as password theft and data loss are relevant to an organization's information assets but not necessarily to a particular employee. In fact, Johnston et al. found that threat appeals can more effectively influence compliance intentions when they emphasize personal relevance [54].

*A possible intention-behavior gap.* Behavioral intention is often used as a proxy for protection motivation and is considered a reasonable predictor of behavior according to the Theory of Planned Behavior [2]. However, prior work has revealed a possible intention-behavior gap, calling for measuring both variables when possible. For example, a meta-analysis of experimental evidence showed that a medium-to-large-sized change in intentions led to only a small-to-medium-sized change in behavior [121]. As people strive to enact their intentions, they may fail to get started, keep goal pursuit on track, or bring goal pursuit to a successful close [93]. Correspondingly, there are self-regulatory mechanisms that help people stick to their intentions, such as forming implementation intentions [35] and monitoring goal progress [41].

A limited number of studies have examined the intention-behavior gap in security contexts. Crossler et al. found that the costs of implementation could be a strong deterrent to full compliance for employees to follow Bring Your Own Device policies [18]. Similarly, Jenkins et al. found that users' desire to minimize required effort negatively moderates the relationship between positive intentions and actual security behavior [50]. On PMT's application in the context of secure mobile payments, Story et al. measured intention and behavior with a one-week gap in between, finding that nudges based on PMT and implementation intention helped translate intention into actual behavior [99]. However, none of these studies has investigated whether PMT-based interventions have triggered permanent and habitual behavioral changes. Our way of measuring the intention-behavior gap is similar to that of Story et al. [99], but future work can adopt a more longitudinal evaluation of the actual behavior.

Altogether, our study contributes to the PMT literature by (1) applying PMT to encourage protection motivation in a new context, i.e., changing passwords after data breaches; (2) separating threat and coping appeals to understand their relative effectiveness; and (3) measuring both intention and behavior to get a complete picture of protection motivation.

## 2.2 Password Policies, Behaviors, and Interventions

*Password policies.* Service providers use password composition policies to prevent users from creating easily guessed passwords [92], as strong passwords, measured by length and complexity, are harder to crack than shorter and simpler passwords [36]. However, there are inconsistencies in the provided guidelines. For example, the US National Institute of Standards and Technology has an eight-character minimum length requirement [36], whereas the UK National Cyber Security Center recommends using at least three random words [106]. Many service providers go further to require different character classes in the password or periodic password changes [16]. Nonetheless, research has shown that it is better to require longer passwords with fewer composition requirements [91], as users circumvent the character class requirements in predictable ways [113].

Research of password corpora has also identified characteristics of common passwords. According to an analysis of leaked passwords from RockYou, the most popular passwords were "123456," "password" and "iloveyou" [116]. Other prevalent semantic themes in passwords include names, locations, dates, animals, and money [72, 117].

We reconcile inconsistencies in existing password requirements and identify the common grounds: a good password policy should require a minimal length and some but not too many classes of special characters, highlight common phrases to avoid, and remove arbitrary password expiration periods. We incorporated such information as well as common passwords to avoid when developing our coping appeal.

*User behaviors.* Despite good-faith efforts in protecting the security of their personal information, most users struggle to comply with password policies [91] and create weak passwords [37, 78, 113]. Password reuse is prevalent [20, 28, 78]: Das et al. estimated that 43-51% of users reuse the same password across multiple sites in their study [20], and Pearman et al. found that the rate would be higher when taking partial reuse into account [78]. Password reuse becomes more likely as more passwords are created or when the reused password is short and simple to memorize [32]. Users match password strength to the account's relative importance [113] and rarely change their passwords unless they forget about the password [98].

Even with external stimuli, users do not always comply with password change advice. Thomas et al.'s work on breached credentials found that only 26% of the warnings resulted in users migrating to a new password [105]. In Bhagavatula et al.'s study based on real-world password data, only 33% of all participants who had accounts on the breached site changed their passwords, and only 13% did so within three months of the breach announcement [8]. In a case study of LinkedIn, Huh et al. found that less than half of participants changed their LinkedIn password upon receiving the password reset notification from the company [45]. For users who change the breached passwords, they rarely change the same or similar passwords on other sites [8], and their new passwords tend to be similar to their old ones [34]. Trust issues can also arise with third-party advice providers. In studying users' perceptions of Chrome's compromised credential notifications, Huang et al. found that some participants falsely assumed Chrome learns about users' plain-text credentials or expressed privacy concerns about Google's management of users' data [44].

Methodologically, prior research has measured password behaviors by tracking participants' log data [8, 28, 30], analyzing passwords from public or private datasets [20, 70], observing password creation in-situ [113], and relying on participants' self-reported data [34, 45, 120]. We evaluate our interventions based on participants' self-reported data, which could still be prone to social desirability and recall biases. However, our method is grounded in high ecological validity as we present participants with real-world breaches that affect their personal data.

*Helping users with passwords.* Password managers are tools that combine secure password storage and retrieval with random password generation to help users deploy strong, unique passwords without memorability issues [79]. However, users are often uncertain about what password managers are, how to use them, and whether they are trustworthy [5, 79, 82, 98]. Alkaldi et al. studied how to encourage the adoption of password managers by satisfying users' self-determination needs in terms of autonomy, relatedness, and competence [6].

Other research has sought to develop nudges that help users create stronger passwords in general. The nudge can be visual or text indicators that provide feedback on the password's strength [12, 112], an estimate of how long it would take to crack the password [115, 123], or social nudges that compare the strength of the user's password with others [24]. Peer et al. showed that password nudges could be more effective when they are also personalized to individuals' decision-making style [80].

Our study expands prior literature by examining the applicability of PMT in encouraging better password behaviors. Compared to nudges, which subtly guide people's behavior without restricting their choices [101], our interventions are more like messaging [56] in that they more explicitly seek to influence the user's decision through information.

## 3 METHOD

Between July and August 2022, we conducted an online experiment to evaluate the effectiveness of PMT-based interventions in encouraging people to change passwords after data breaches. Our study was approved by the Institutional Review Boards at the University of Michigan and the George Washington University.

To increase the ecological validity of our evaluation, we drew on Mayer and Zou et al.'s methodology [69] and pulled participants' breach records from Have I Been Pwned (HIBP) using its public API, thereby situating our interventions in real-world breaches known to affect individual participants. HIBP is a database maintained by security expert Troy Hunt who routinely analyzes password dumps and text storage sites on the Internet to collect information about leaked account credentials. As of August 2022 (when we finished data collection), the site listed 622 breached websites with over 11 billion breached accounts.

### 3.1 Study Design

The purpose of our study is to evaluate to what extent PMT-based interventions are effective at encouraging consumers to change their passwords after being affected by a data breach. The key dependent variables are participants' self-reported password-change intentions and behaviors. Our experiment examines the effect of threat and coping appeals together and in isolation, with four conditions:

- Control: Participants were not presented with any threat or coping-related information. As a baseline, participants were still presented with a prompt: "We recommend that you change the password for your [site name] account" as well as information about a data breach that affected them. This baseline prompt appeared in all conditions.
- Threat appeal only: Participants were presented with information about the risks associated with passwords being leaked in a data breach and how the risks could affect them personally (see Figure 1).
- Coping appeal only: Participants were presented with information about how to change their password, how changing the password reduces the threat, and estimated time to change their password (see Figure 2).
- Threat and coping appeals: Participants were presented with the combined information about both threat and coping described above.

We drew on existing literature to design our interventions. The threat appeal (1) features negative things that could happen to affected users when a data breach involves login credentials [34, 104] (targeting *perceived severity*) and (2) addresses optimism bias and hyperbolic discounting that people may experience after data breaches [55, 128] (targeting *perceived vulnerability*). The coping appeal (1) builds the connection between changing the password and reducing the chance of account compromise (targeting *response efficacy*), (2) gives a list of concrete steps to take, including a URL to the breached site and guidelines about how to create strong passwords [19] (targeting *self-efficacy*), and (3) highlights that the effort "only takes a few minutes" and is "easy" (targeting *response costs*). In line with prior work's recommendations [17, 25, 44], we followed a layered approach in presenting the text to reduce participants' cognitive load while nudging them to pay attention. Participants would have to check out the full text by clicking through multiple interactive expandable boxes (with a short delay between boxes) before being able to proceed to the next page.

The experiment was carried out through three online surveys (see Figure 3 for an overview and Appendix A for full survey questionnaires). In the screening survey, we obtained participants' consent and asked them to provide an email address to be queried in HIBP for all breach records associated with that email address. We determined each participant's eligibility based on the query

> **What are the risks**
> - Criminals may access your account to steal your personal information, impersonate you, or make fraudulent purchases in your name.
> - If you used the same password elsewhere, criminals may take over your other accounts too.
> - Criminals use automated programs to test compromised passwords on hundreds of accounts in just a few seconds. You're at risk regardless of whether you are a promising target or not.
> - Once your password is out there, criminals may try to take over your account anytime after a breach, no matter how long ago the breach happened.

Fig. 1. The threat appeal we used in our study.

> **How to change your password** Changing your [site name] account password would prevent criminals from using the breached password to access your account. It only takes a few minutes. Just follow these easy steps:
> (1) **Go to [site URL] and log into your account.**
>     Unsure if you have a [site name] account or can't log into it? Contact [site name] to recover the account or have your account deleted. You can usually find contact information in the privacy policy.
> (2) **Create a unique and strong password in account settings.**
>     Longer passwords are best. Do not reuse the same password for other accounts. Check out this guideline [19] for more do's and don'ts about passwords.
> (3) **You're all set!**
>     If you used your old password for other accounts, make sure to change your password for those accounts too.

Fig. 2. The coping appeal we used in our study.
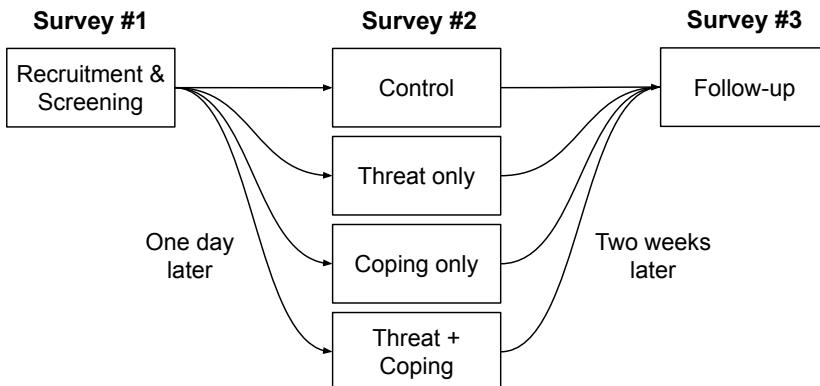


Fig. 3. An overview of our experiment's procedure.

results and invited eligible participants back for the main survey. In the main survey, participants were presented with different nudging text based on the condition they had been randomly assigned to and were asked to report their password change intention. For participants who indicated the password had not been changed since the breach (Q25) — meaning that the password needs to be changed — we invited them back two weeks later for a follow-up survey that measured whether they had changed the password after receiving the intervention.

## 3.2   Protocol

*Pilot testing.* To ensure that the interventions we developed worked as intended the first author conducted four cognitive walkthrough sessions [62] with participants recruited through convenience sampling (see Appendix B for the protocol). All four participants confirmed that the text was intuitive and aligned with their understanding of threats related to breached passwords and challenges regarding changing passwords. We made minor tweaks to the questionnaire, then conducted a second round of pilot testing with a larger sample recruited via Prolific.[1] We made further changes to the questionnaire design, and used the pilot data to determine participants' compensation and effect sizes to be considered in power analysis (more in Section 3.3).

*Recruitment & Data Collection.* We recruited participants for the screening survey via Prolific. We made our screening survey open to prospective participants who spoke English, were at least 18 years old at the time of the survey, and were living in the United States. We also limited the survey to participants who could take it in Chrome/Firefox on a desktop computer, since we found through pilot testing that our survey infrastructure ran into occasional technical issues in other environments.

We began collecting data for the screening survey in July 2022 and concluded data collection for the follow-up survey in August 2022. We obtained 2,412 complete responses to the screening survey. In creating our sample, we sought a diverse representation of gender, age, and educational attainment. Specifically, we used the "balanced sample" feature on Prolific, which allows us to distribute the study evenly to male and female participants.[2] Furthermore, we released slots for the screening survey in small batches ($n \approx 100$), monitored the demographic distributions of incoming data, and used Prolific's pre-screeners to balance age and education as needed.

The actual experiment began with the main survey and continued through the follow-up survey. Among participants who completed the screening survey, 1,824 (75.6%) were deemed eligible. We invited these participants back for the main survey one day after they completed the screening survey. Among the 1,654 (90.7%) participants who returned and completed the main survey, 1,388 (83.9%) selected "yes" or "no" for the password change intention question, and the remaining 266 (16.1%) selected "already changed."[3] We excluded participants who selected "already changed" from the follow-up survey and from our data analysis since the intervention would not apply to them as there is no need for them to change their password again. Among participants who received the follow-up survey invitations, 1,176 (84.7%) returned and completed the follow-up survey.

Aiming to compensate participants at least $15/hour, we set the compensation accordingly: $0.80 for the screening survey, $2.40 for the main survey, and $1.00 for the follow-up survey. The actual median completion times were 1.84 minutes (screening), 6.64 minutes (main), and 3.71 minutes (follow-up), corresponding to a rate of $26.08/hour, $21.69/hour, and $18.76/hour respectively.

*Screening Survey.* After obtaining their informed consent, we asked participants to provide an email address. We used the email address to query the HIBP database and obtain a list of breaches in which the participant's email address was exposed. We informed participants that the querying task would be completed in a privacy-preserving manner: by keeping participants' email addresses in ephemeral storage and deleting them after the query had been sent, we never had direct exposure to participants' email addresses, nor did we store them anywhere or include them in our analysis.

---

[1]We collected 107, 76, and 69 complete responses for the screening, main, and follow-up surveys, respectively. Each participant was compensated $1.00, $3.00, and $1.60 for completing each survey respectively.

[2]While Prolific uses sex as one of its pre-screener variables, we used gender in our questionnaire, also including "non-binary," "prefer to self-describe," and "prefer not to say" options.

[3]Participants who selected "already changed the password" for the intention question were almost evenly distributed across the four conditions (X: 61/22.9%; T: 73/27.4%; C: 69/26.0%; CT: 63/23.7%).

Participants who were uncomfortable with providing their email addresses could opt out. Among the 2,625 participants who consented to participate in the study, 172 (6.6%) opted out when asked to provide an email address.

For participants who provided an email address, we queried HIBP and informed them of their eligibility for our experiment. A participant would be eligible only if they provided an email address for their own email account. Furthermore, the participant needed to have at least one valid breach for their provided email address. We considered that a breach is valid (1) if passwords were among the types of breached information, which makes changing the password a reasonable option, and (2) changing the password is indeed a viable option on the breached site, meaning that the site should be functioning, have an account creation feature, and conduct business with average consumers rather than other businesses.[4] Participants who were ineligible for our study were redirected to the final page showing the breach records associated with their provided email addresses.

For eligible participants, we asked them to indicate how they used the email account and collect demographic information at the end of the screening survey, as these are all possible covariates of one's password change behaviors. For the email-related questions, we drew on the same set used in Mayer and Zou et al. [69], including how often they checked this email account, how long it has been used, and what they used the account for. We further asked participants about the value of created accounts (low, medium, or high, with examples provided for each category).

*Main Survey.* For participants who passed the screening, we sent invitations to the main survey one day later. The main survey started by showing a breach that involved passwords randomly chosen from their breach records. We provided a short description of the breach, the site's logo and name, and the types of compromised data, all drawing from HIBP. We highlighted passwords being compromised and listed other data types as "additional information" (see Figure 4). We then asked participants about their awareness in three dimensions: whether they had heard of the site, whether they had known they were affected by the breach, and whether they had an account with the site. For those with an account, we further asked them to specify their account usage, including the account's age, frequency of use, and perceived importance.

Next, we randomly assigned participants to one of the four conditions: all conditions included the password change prompt, but participants in the treatment conditions received additional information targeting threat appraisal, coping appraisal, or both. After showing the intervention, we asked participants to indicate their password change intention ("yes" "no" "already changed") and to explain their choice in a text box. We also asked participants whether they had used the breached password for other online accounts.

Following the password reuse question, we asked participants a series of Likert questions to assess five PMT constructs – perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response costs – using scales adapted from prior work for each construct [9, 99]. We used these responses as manipulation checks to gauge how effective our interventions were at targeting our participants' threat and coping appraisals. We also included two attention-check questions. The main survey ended with questions about the participant's security attitudes and prior negative experiences adapted from prior literature [27, 129] as additional covariates of password change intention and behavior.

*Follow-up Survey.* For participants who were eligible for the follow-up survey, we sent out the invitation two weeks after they completed the main survey. We decided on the two weeks timeframe

---

[4]To ensure the second criterion is met, we manually inspected all breached sites listed in the HIBP database in June 2022, right before launching the experiment. Our manual filtering led us to exclude 230 out of the 598 breaches (38.5%) in the HIBP's database at the time of our study.

Fig. 4. Example breach information shown to participants.

based on pilot testing, as all pilot participants who ended up changing their password did it within two weeks. We believe that this timeframe gave participants enough time to change their password but was not too long to cause recall issues.

The follow-up survey began by reminding participants of the previous surveys they took and the breach featured. Next, we asked participants to describe in free text what they had done in response to learning about the breach, followed by an attention check asking participants to select the name of the featured breach. We then asked participants to specify whether they had changed their password since taking the main survey, why, and what they did to passwords for other accounts. Those who indicated they had changed their password since taking the main survey were asked to provide more details, such as when they changed the password and what mechanisms they used to remember the new password.

Participants could further optionally upload a screenshot of the password reset confirmation email. We adopt this approach from Huh et al. [45] as a measure to validate participants' self-reported behavior and set a $1.00 bonus payment for those who uploaded a valid screenshot. Importantly, the screenshot upload prompt (Q46) came after the question that asked participants whether they actually changed their password (Q40), and participants were not allowed to go back and change their earlier responses. In this sequence, we ensured that participants' reported password change behaviors occurred as a result of our intervention rather than the additional monetary incentive.

## 3.3 Data Analysis

We pre-registered our study protocol, hypotheses, and data analysis plan prior to data collection on Open Science Framework.[5]

*Hypotheses.* Our key independent variable is the condition: control (X), threat only (T), coping only (C), and threat and coping combined (CT). Our key dependent variables are participants' intention and self-reported action to change their breached passwords. Because the four conditions had different amounts of threat- and coping-related information, and because the control condition does not have any threat or coping information, we made the following hypotheses for password change intention:

**H1**: There is a significant association between the condition and whether or not the participant would intend to change their breached passwords.

- **H1a**: Participants in the control condition will exhibit lower password change intentions than those in the threat-only condition. (*intention: X<T*)
- **H1b**: Participants in the control condition will exhibit lower password change intentions than those in the coping-only condition. (*intention: X<C*)
- **H1c**: Participants in the control condition will exhibit lower password change intentions than those in the threat+coping condition. (*intention: X<CT*)

Assuming that the intervention's effect on intention in the main survey carries over into the follow-up survey, we made the following hypotheses for password change behavior:

**H2**: There is a significant association between the condition and whether or not the participant would end up changing their breached passwords.

- **H2a**: Fewer participants in the control condition will end up changing their breached passwords than those in the threat-only condition. (*behavior: X<T*)
- **H2b**: Fewer participants in the control condition will end up changing their breached passwords than those in the coping-only condition. (*behavior: X<C*)
- **H2c**: Fewer participants in the control condition will end up changing their breached passwords than those in the threat+coping condition. (*behavior: X<CT*)

We did not plan to apply p-value corrections for the pairwise comparisons since our hypotheses are confirmatory rather than exploratory. In addition, we did not include directional hypotheses regarding differences among the three treatment conditions because prior work has not provided sufficient evidence on whether the threat or coping appeals may be more effective or whether the two appeals combined would be more effective than each presented in isolation [66, 114]. However, we were still interested in understanding their differences, and we ran additional pairwise comparisons as exploratory analyses to obtain insights.

*Data Cleaning.* We retained all complete responses for the screening survey. We used the attention checks in the main and follow-up surveys to flag responses that required further examination. Among the 1,388 participants who completed the main survey — excluding those who already changed passwords — 32 failed one of the attention checks, and two failed both attention checks. Among the 1,176 participants who completed the follow-up survey, one failed the attention check. We excluded responses from the two participants who failed both attention checks in the main survey and the one who failed the attention check in the follow-up survey. We retained the remaining responses since the data for other parts of the survey was detailed and insightful. We also retained responses from the 211 participants who completed the main survey but did not complete the follow-up survey since they still contributed insights for half of our key hypotheses.

---

After data cleaning, the number of complete and valid responses for the main survey was 1,386 — we regard this as the final sample size of our study. The distribution across conditions is almost even for the main survey (control: 349/25.2%; threat-only: 339/24.5%; coping-only: 348/25.1%; threat+coping: 350/25.2%) and the follow-up survey (control: 291/24.8%; threat-only: 304/25.9%; coping-only: 297/25.2%; threat+coping: 283/24.1%).

*Statistical Analyses.* To examine H1 and H2, we conducted two omnibus $\chi^2$ tests: both tests used the condition assigned (four levels) as the independent variable, intention (yes/no, excluding "already") and action (yes/no) as the dependent variable, respectively. To examine H1a-H1c and H2a-H2c, we conducted pairwise $\chi^2$ comparisons to detect the differences between the control and any treatment conditions. Following practices in prior work [99], we planned to run these pairwise comparisons regardless of the omnibus test results since we had solid and theory-informed hypotheses that any treatment would better encourage password changes than the control condition.

We also planned and conducted a series of exploratory analyses. To gather insights into the relative performance of threat versus coping appeals, we conducted pairwise comparisons between the three treatment conditions. To understand to what extent the threat and coping appeals address participants' threat and coping appraisals respectively, we conducted Kruskal-Wallis tests to investigate the relationship between the condition (IV) and each of the five PMT constructs (DV) as manipulation checks.

We were also interested in knowing whether the intervention's effect would remain robust after controlling for other covariates, such as individuals' account usage and demographics. To this end, we built logistic regression models with the condition and other covariates as IVs and intention/action as the DV. To avoid model fit problems caused by too few observations in a category, we binned the demographic data in Table 1 into fewer categories for the regression analyses: gender (binary: men or women), age (three levels: 18-34, 35-54, 55+), educational attainment (three levels: high school or less, some college, Bachelor's degree or above), and annual household income (three levels: <$50k, $50-100k, >$100k). We report odds ratios, confidence intervals, and p-values for regression results.

*Qualitative Analysis.* We analyzed participants' open-ended text responses using thematic coding [89] to gather deeper insights into their reasoning behind password change intention (Q26), what they did in general after learning about the breach (Q38), and reasoning behind password change action (Q41). The first author created an initial codebook and sought feedback from the research team in multiple discussions to iteratively improve the codebook. Since our analysis seeks to report quantitative analysis of qualitative data (e.g., that a theme showed up in X% of our data), the first author then worked with the second author to double-code 20% of responses to ensure sufficiently high inter-rater reliability [71]. Cohen's $\kappa$ was consistently above 0.80 across three rounds of comparison, and the final values were 0.83 for Q26, 0.88 for Q38, and 0.86 for Q41. After that, the first and second authors resolved coding discrepancies through discussions, and the first author went back to review all responses using the finalized codebook (Appendix E).

*Power Analysis.* We conducted an *a priori* power analysis to determine our target number of participants based on effect sizes observed in the pilot data. Our pilot data suggested a small-to-medium effect ($w$=0.15) for the omnibus $\chi^2$ test on intention and a small effect ($w$=0.10) for pairwise comparisons on intention. We based our power analysis on pairwise comparisons since we wanted to ensure we would have enough data to detect between-condition differences. For 80% power at $\alpha$=0.05 and $df$=1, G*Power suggested we need 1,570 participants in total for the main survey. We did not achieve this goal due to budgetary constraints and an underestimation of participants whose data got excluded from the analysis because they had changed the password already (16% of

| Metric | Sample | Census |
|---|---|---|
| Women, Men, Non-binary | 50.9%, 46.5%, 1.9% | 51%, 49%, n/a |
| 18-24, 25-34 years | 16.0%, 22.9% | 7%, 14% |
| 35-44, 45-54 years | 21.5%, 19.5% | 13%, 13% |
| 55-64, 65 years or older | 13.3%, 5.4% | 13%, 15% |
| High school or less, Some college | 11.6%, 23.7% | 37%, 15% |
| Associate's degree (aca./voc.) | 11.8% | 11% |
| Bachelor's degree | 36.9% | 24% |
| Advanced degree (Master's/professional/doctoral) | 15.7% | 14% |
| <$25k, $25k-$50k | 16.0%, 22.3% | 19%, 20% |
| $50k-$75k, $75k-$100k | 20.1%, 14.9% | 16%, 12% |
| $100k-$150k, >$150k | 13.5%, 10.0% | 14%, 19% |
| Asian, Black | 7.8%, 6.8% | 6%, 14% |
| White, Two or more races | 76.9%, 5.0% | 76%, 3% |
| Hispanic/Latino | 9.8% | 19% |
| Other (e.g., American Indian, Pacific Islander) | 0.9% | 2% |

Table 1. Gender, age, education, income, race/ethnicity compositions among participants of the main survey ($n$=1,386). Census statistics from [107–110] as of 2022. Some percentages do not add up to 100% due to non-reporting.

all completed main survey responses, whereas our original estimate was 5%). However, our final sample size still enabled us to detect a small effect for the omnibus $\chi^2$ test ($w$=0.09 for intention; $w$=0.10 for action) and a small-to-medium effect for the pairwise comparisons ($w$=0.11 for intention; $w$=0.12 for action).

## 4 QUANTITATIVE RESULTS

In this section, we summarize participant demographics and breaches featured in our study, present key findings in relation to our hypotheses, then present manipulation check and regression results to contextualize and interpret the differences between conditions.

### 4.1 Sample

*Participant profile.* Table 1 summarizes the demographics of our main survey participants compared to the US census bureau's data. Our sample has a quite balanced distribution of gender, income, and race/ethnicity, but it is slightly more educated and younger than the US population. A minority of participants reported having studied or worked in computer science/information technology (314; 22.7%), and fewer reported having studied or practiced law or other legal services (49; 3.5%).

We asked participants how they used the email account they provided for our study. Most participants used the email for an extended period (mean: 12.81 years, median: 12). Most participants checked the email daily (85.4%); the rest checked the email weekly (11.7%), monthly or less frequently (2.9%). In addition, participants could choose multiple options for what they used the email for. Most participants selected using the email account for personal correspondence (86.4%), followed by signing up for medium-value accounts (75.0%), signing up for sensitive accounts (57.4%), signing up for low-value accounts (53.1%), and professional correspondence (40.8%). These results indicate that participants were checking breach records for email accounts that they used regularly and for important purposes, which adds to our findings' ecological validity.

*Overview of breaches.* We showed each participant information about a real-world password breach associated with their email address, randomly selected from their breach records provided by HIBP. Our sample consists of 127 unique breaches. The most frequently shown breaches came from Zynga (141), MyFitnessPal (128), MySpace (65), and Chegg (62). Figure 5 in Appendix C gives a more complete overview of breaches in our sample. Aside from email addresses and passwords, which were exposed in every breach due to our study design, the other most commonly breached data types included names (63), IP addresses (54), and dates of birth (35). For other types of data that got leaked in our sample's breaches, see Figure 6 in Appendix C. We also calculated breach age, defined as the time between the breach's occurrence date and the survey's completion date. The average age of breaches in our sample was 5.16 years (median: 4.2, sd: 3.13).

## 4.2 Comparisons Between Experimental Conditions

A majority of participants (868, 62.6%) in the main survey stated they intended to change the breached password. However, only about a third (320, 27.2%) reported having changed the password in the follow-up survey. The substantial drop from intention to action suggests that there is an intention-behavior gap in individuals' reactions toward the advice about changing breached passwords, and our qualitative results in Section 5 provide insights into why.

Looking at the descriptive statistics, we observed the following trends: *threat only* > *coping only* ≥ *threat + coping* > *control* for motivating password intention; *threat + coping* > *threat only* ≥ *coping only* > *control* for motivating actual password changes. However, the differences between groups were minor, which might explain why for the two omnibus $\chi^2$ tests of independence we conducted on intention and action respectively, both tests led to non-significant results ($\chi^2(3)$=6.10, $p$=.11 for intention; $\chi^2(3)$=5.27, $p$=.15 for action). As such, we rejected both H1 and H2: there was no significant association between the conditions participants were assigned to and whether or not they intended to change, or actually changed their breached passwords.

While the omnibus $\chi^2$ test results were non-significant, we ran pairwise $\chi^2$ tests of independence to test the confirmatory directional hypotheses we developed about the differences between the control and treatment conditions. Significant differences were found for specific pairs, summarized in Tables 2 and 3. Participants who saw the threat appeal alone were 1.48x more likely to intend to change their breached password than the control condition ($p$=.02), confirming H1a. Participants who saw both the threat and coping appeals were 1.54x more likely to change their breached password than the control condition ($p$=.02), confirming H2c. The odds ratio for both comparisons only corresponds to a small effect size [13]. We did not find a statistically significant difference between *coping only* vs. *control* for intention ($p$=.23), between *threat + coping* vs. *control* for intention ($p$=.30), between *threat only* vs. *control* for action ($p$=.14), or between *coping only* vs. *control* for action ($p$=.23). H1b, H1c, H2a, H2b are rejected. These results show that, compared to the control condition, threat appeal alone was more effective at increasing password change intention. However, participants were the most likely to act only when both threat and coping appeals were present.

As part of our exploratory analyses, we ran pairwise $\chi^2$ tests between the three treatment conditions. For intention, we did not observe any significant differences between *threat only* vs. *threat + coping* ($p$=.20), *coping only* vs. *threat + coping* ($p$=.92), or *threat only* vs. *coping only* ($p$=.27). The same pattern of non-significant pairwise difference also applies to action: $p$=.46 for *threat only* vs. *threat + coping*, $p$=.31 for *coping only* vs. *threat + coping*, and $p$=.85 for *threat only* vs. *coping only*. These results confirm the pattern in Tables 2 and 3: the differences in motivating password changes between the three treatment conditions were minor (1% to 4% based on descriptive statistics) and were not significant even with a large enough sample to detect a small-to-medium effect.

| Conditions | % w/ intention | OR | 95% CI | p-value |
|---|---|---|---|---|
| Threat only vs. Control | 67.3% vs. 58.2% | 1.48 | [1.07, 2.04] | .02 |
| Coping only vs. Control | 62.9% vs. 58.2% | 1.22 | [0.89, 1.68] | .23 |
| Threat + Coping vs. Control | 62.3% vs. 58.2% | 1.19 | [0.88, 1.63] | .30 |

Table 2. Pairwise comparisons between control vs. treatment for the percent of participants who reported intending to change the password in the main survey.

| Conditions | % w/ action | OR | 95% CI | p-value |
|---|---|---|---|---|
| Threat only vs. Control | 28.0% vs. 22.7% | 1.32 | [0.90, 1.95] | .14 |
| Coping only vs. Control | 27.3% vs. 22.7% | 1.29 | [0.86, 1.90] | .23 |
| Threat + Coping vs. Control | 31.1% vs. 22.7% | 1.54 | [1.04, 2.27] | .02 |

Table 3. Pairwise comparisons between control vs. treatment for the percent of participants who reported having changed the password in the follow-up survey.

## 4.3 Manipulation Checks

Table 8 in Appendix D shows the descriptive statistics of participants' ratings of the five PMT constructs: threat severity, threat vulnerability, response efficacy, self-efficacy, and response costs. To understand to what extent our interventions produced the intended effect on participants' threat and coping perceptions, we conducted Kruskal-Wallis tests to detect whether participants' ratings of each construct differed between conditions, followed by post hoc Dunn tests to detect significant differences between any pairs. We applied Holm-Bonferroni correction to the post hoc Dunn tests to control for Type I error due to the exploratory nature of the analysis.

Results of the Kruskal-Wallis tests showed that our interventions had different effects on participants' perceived threat vulnerability ($H(3)=14.11$, $p=.002$) and perceived response efficacy ($H(3)=21.52$, $p<.001$). The post hoc Dunn tests further revealed that participants who received the threat appeal had significantly higher ratings of perceived threat vulnerability, evidenced by the significant differences between threat-only vs. control ($p=.01$) and threat+coping vs. control ($p=.004$). Interestingly, the threat appeal also seemed to increase participants' coping perceptions. Participants who received the threat appeal had significantly higher ratings of response efficacy, evidenced by the significant differences between *threat only* vs. *control* ($p=.009$), *threat + coping* vs. *control* ($p<.001$), and *threat + coping* vs. *coping only* ($p=.009$). There was no significant difference between conditions for participants' ratings of threat severity ($H(3)=0.97$, $p=.81$), self-efficacy ($H(3)=1.30$, $p=.73$), or response costs ($H(3)=4.06$, $p=.26$); the post hoc Dunn tests did not reveal any significant pairwise differences for these three variables.

These results suggest that our interventions' targeting of PMT constructs were somewhat but not fully successful. The threat appeal primarily influenced participants' threat perception by influencing perceived threat vulnerability. In addition, the threat appeal's presence strengthened participants' perception of response efficacy, even though response efficacy is part of coping appraisal according to PMT, whereas the presence of coping appeal alone did not help much. This could mean that our coping appeal did not produce desired effects on participants' coping appraisals. Another possible explanation is that particular challenges associated with changing breached passwords make a coping appeal inapplicable — some participants could not find an

account with the breached site to start with; other participants tried the "forget my password" feature but never received a password reset confirmation email. We provide more details about these challenges in Section 5.

## 4.4 Other Factors Related to the Breach and Affected Account

In the main survey, we asked participants to report their awareness of the company/breach, security attitudes, prior negative incidents, as well as how they used the online account affected by the breach. We treat these factors as covariates that could impact their password change behaviors in addition to the condition they were assigned to.

*Aware of the company, but not the breach.* For prior awareness (Q16, Q17), the majority (75.8%) of participants had heard of the breached site before our study, 17.1% had not, and 7.1% were unsure. By contrast, the majority (82.3%) of participants were unaware that they were affected by the breach we showed them before our study, 7.0% had known they were affected, and 10.8% were unsure.

*Most affected accounts were rarely used and perceived as unimportant.* We further asked participants whether they had an account with the breached site (Q18), hypothesizing that password change would only be actionable, and thus more likely, for those with an account.[6] More than half of participants indicated they had created an account with the breached site, either by providing an email address and a password (48.5%) or by using a social login feature such as "sign in with Google" or "sign in with Facebook" (6.9%). The rest did not think they had an account (16.6%) or were unsure about the account's existence (28.1%).

For participants who reported having an account with the breached site, we followed up with questions about the account's age (Q20), frequency of use (Q21), and perceived importance (Q24). Most accounts had existed for an extended period (mean: 5.98 years; median: 5; sd: 4.36). Most participants (87.2%) logged into the account only yearly or even less frequently; the rest checked the account monthly (8.0%), weekly (3.5%), or daily (1.3%). When asked about the account's perceived importance, most participants indicated that the account was "very unimportant" (51.1%) or "unimportant" (23.1%) to them. Average ratings of the perceived importance level were low (mean: 2.04; median: 1; sd: 1.44 for a 7-point scale), which might be due to a non-trivial amount of participants not knowing whether they had an account with the breached site. Altogether, these results illustrate the nature of accounts affected by HIBP breaches among our sample: most participants created the account a while ago, only used it very infrequently, and did not attach much value to the account.

*Low rate of password reuse for affected accounts.* Excluding 11.0% of participants who claimed they did not have an account with the breached site, 12.3% knew for sure they used the breached password elsewhere, 32.5% did not reuse the breached password, and 44.2% were unsure. The low rate of participants who reused the breached password for other accounts matches the finding of most affected accounts being unimportant, as prior work has found that users tend to reuse passwords that they have to enter frequently [119].

*Other covariates.* We examined participants' security attitudes using SA-6 [27] (Q33) and prior experience with account compromise (Q34), data breach (Q35), and identity theft (Q36) as background variables that do not relate to any specific breach or online account, but could still impact participants' overall security posture. Most participants' SA-6 ratings were between the medium to high end (mean: 3.44; median: 3.75; sd: 0.95), indicating that most participants were fairly motivated

---

[6]In Q22 and Q23 we also asked participants to select what types of information the account might have about themselves. However, only in the middle of data collection did we find out that Q22 did not have a "none of the above" option, and participants could not skip this question. As such, we refrain from reporting the results of this question since the responses were likely skewed due to the survey question's design.

to learn about security and follow expert-recommended advice. More than half of the participants knew that their information was exposed in other data breaches before our study (57.2% yes; 36.1% no; 6.6% unsure). Fewer participants had experienced account compromises (29.1% yes; 54.6% no; 16.3% unsure) or identity theft (12.0% yes; 81.4% no; 6.6% unsure).

## 4.5 Regression Results

Having understood participants' awareness of the breach and usage of the affected account through descriptive statistics, we next ran logistic regressions to compare the intervention's effect with other covariates. We included the same set of independent variables for the intention model (Table 4) and action model (Table 5): experimental condition, prior knowledge of the breached site, prior knowledge of the breach, account existence, reuse of the breached password, security attitudes (SA-6), prior negative experience (with account compromise, data breach, and identity theft), demographics (age, gender, education, income), and the breach's timing.

*Treatment vs. control differences hold after controlling for covariates.* We found that participants who saw the threat appeal were still more likely to form password change intention than those in the control condition ($OR$=1.84, $p$=.01). Similarly, the significant difference between the *threat + coping* condition and *control* condition still holds for password change action ($OR$=2.18, $p$=.006). The regression results also suggest that participants in the *threat only* condition were more likely to end up changing their passwords compared to the control condition ($OR$=1.83, $p$=.02). However, because the $\chi^2$ pairwise comparison does not yield significant results, the difference between the two is inconclusive.

*Proactive security attitudes contribute to changing passwords.* Participants who held more proactive security attitudes, reflected by higher SA-6 ratings, were significantly more likely to both form password change intentions ($\beta$=0.65, $p$<.001) and end up changing their passwords ($\beta$=0.46, $p$<.001). Our findings contradict some other studies in which SA-6 did not explain variances in their outcome variables, such as using secure mobile payments [99] and adhering to privacy setting suggestions [58]. A possible explanation is that some of the SA-6 scale items (e.g., "I am extremely motivated to take all the steps needed to keep my online data and accounts safe") are more directly relevant to our study's context.

*Higher likelihood to change passwords for recent breaches.* Breach age, i.e., how long ago the breach happened in years, emerged as a significant predictor in both models. If the breach happened a while ago, participants were less likely to form password change intention ($\beta$=−0.09, $p$=.001) or to end up changing their password ($\beta$=−0.11, $p$<.001). This finding also aligns with prior research on consumer reactions to data breaches in which the occurrence of actual harms was often used as a heuristic for deciding whether to take action [1, 68, 128]: if a breach happened a while ago and nothing happened, consumers may take it as a signal that no action is needed, although the objective risk of leaked data being misused does not decrease over time.

*Predictors for password change intention but not action.* Some predictors, namely whether the breached password was reused elsewhere and the participant's gender and income, could significantly explain the variances in participants' password change intention. Participants who reused the breached password for other online accounts, as well as those who were unsure about the password being reused or not, were significantly more likely to form password change intentions ($OR$=3.01, $p$<.001; $OR$=1.82, $p$=.002). Participants who identified as women were more likely to form password change intentions than men ($OR$=1.97, $p$<.001). Participants with a >100K annual household income were more likely to form password change intentions than those earning <50K

| | B (SE) | OR | 95% CI | p-value |
|---|---|---|---|---|
| (Intercept) | $-2.88(0.59)$ | 0.06 | $[0.02, 0.18]$ | $< .001$ |
| Condition: coping (vs. control) | $0.28(0.24)$ | 1.32 | $[0.83, 2.11]$ | .24 |
| Condition: threat (vs. control) | $0.61(0.24)$ | 1.84 | $[1.15, 2.95]$ | .01 |
| Condition: combined (vs. control) | $0.28(0.29)$ | 1.32 | $[0.82, 2.17]$ | .25 |
| Account exist: yes (vs. no) | $-0.15(0.32)$ | 0.86 | $[0.45, 1.60]$ | .63 |
| Account exist: yes (vs. no) | $-0.28(0.30)$ | 0.75 | $[0.42, 1.37]$ | .35 |
| Aware account: yes (vs. no) | $0.50(0.35)$ | 1.64 | $[0.82, 3.29]$ | .16 |
| Aware account: unsure (vs. no) | $0.15(0.34)$ | 1.17 | $[0.59, 2.28]$ | .65 |
| Password reuse: yes (vs. no) | $1.10(0.31)$ | 3.01 | $[1.66, 5.69]$ | $< .001$ |
| Password reuse: unsure (vs. no) | $0.60(0.19)$ | 1.82 | $[1.25, 2.67]$ | .002 |
| Security attitudes (5-point scale) | $0.65(0.10)$ | 1.92 | $[1.58, 2.34]$ | $< .001$ |
| Acc. Compromise: yes (vs. no) | $0.15(0.20)$ | 1.16 | $[0.79, 1.71]$ | .44 |
| Prior breach: yes (vs. no) | $-0.24(0.19)$ | 0.78 | $[0.54, 1.13]$ | .20 |
| Identity theft: yes (vs. no) | $0.12(0.29)$ | 1.13 | $[0.64, 2.04]$ | .68 |
| Age: 35-54 (vs. 18-34) | $0.29(0.20)$ | 1.33 | $[0.90, 1.96]$ | .24 |
| Age: 55+ (vs. 18-34) | $0.62(0.26)$ | 1.87 | $[1.12, 3.15]$ | .15 |
| Gender: women (vs. men) | $0.68(0.18)$ | 1.97 | $[1.38, 2.82]$ | $< .001$ |
| Edu.: ≥Bach. (vs. ≤high school) | $0.28(0.30)$ | 1.32 | $[0.72, 2.30]$ | .36 |
| Edu.: Some College (vs. ≤high school) | $0.47(0.30)$ | 1.60 | $[0.88, 2.90]$ | .12 |
| Income: 100+K (vs. <50K) | $0.52(0.25)$ | 1.69 | $[1.05, 2.76]$ | .03 |
| Income: 50-100K (vs. <50K) | $0.03(0.20)$ | 1.03 | $[0.69, 1.52]$ | .89 |
| Breach age (years) | $-0.09(0.03)$ | 0.92 | $[0.87, 0.97]$ | .001 |

Table 4. Logistic regression for predicting password change intention in the main survey. $n$=725 after excluding incomplete or not applicable responses. Cox and Snell $R^2$=0.14. Model $\chi^2(21)$=111.05, $p<.001$

($OR$=1.69, $p$=.03). However, these differences no longer held for the action model, and we were unable to conclude confidently about password reuse and demographics being significant predictors.

## 4.6 How Participants Changed Their Passwords

We asked participants in the follow-up survey ($n$=1, 175) whether they changed the password for other online accounts (Q42). For those who indicated they changed the breached password ($n$=319), we further asked how soon they changed the password since taking the main survey (Q43), what they used for the new password (Q44), and what techniques they used for remembering the new password (Q45) to characterize their password change behaviors, using survey questions from prior work [34, 67].

| | B (SE) | OR | 95% CI | p-value |
|---|---|---|---|---|
| (Intercept) | $-2.98(0.68)$ | 0.05 | [0.01, 0.19] | < .001 |
| Condition: coping (vs. control) | 0.46(0.28) | 1.59 | [0.92, 2.74] | .10 |
| Condition: threat (vs. control) | 0.60(0.26) | 1.83 | [1.10, 3.09] | .02 |
| Condition: combined (vs. control) | 0.78(0.28) | 2.18 | [1.26, 3.83] | .006 |
| Aware site: yes (vs. no) | 0.18(0.36) | 1.20 | [0.59, 2.47] | .62 |
| Aware breach: yes (vs. no) | 0.22(0.32) | 1.24 | [0.66, 2.31] | .49 |
| Account exist: yes (vs. no) | 0.42(0.40) | 1.52 | [0.70, 3.42] | .30 |
| Account exist: unsure (vs. no) | 0.17(0.40) | 1.05 | [0.69, 1.58] | .66 |
| Password reuse: yes (vs. no) | $-0.03(0.30)$ | 0.97 | [0.53, 1.75] | .93 |
| Password reuse: unsure (vs. no) | 0.05(0.21) | 1.05 | [0.69, 1.58] | .83 |
| Security attitudes (5-point scale) | 0.46(0.11) | 1.59 | [1.28, 1.99] | < .001 |
| Acc. Compromise: yes (vs. no) | $-0.10(0.21)$ | 0.90 | [0.59, 1.37] | .63 |
| Prior breach: yes (vs. no) | $-0.05(0.20)$ | 0.95 | [0.64, 1.43] | .82 |
| Identity theft: yes (vs. no) | 0.36(0.29) | 1.44 | [0.81, 2.52] | .21 |
| Age: 35-54 (vs. 18-34) | $-0.37(0.22)$ | 0.69 | [0.44, 1.06] | .09 |
| Age: 55+ (vs. 18-34) | 0.33(0.27) | 1.39 | [0.83, 2.34] | .21 |
| Gender: women (vs. men) | $-0.06(0.19)$ | 0.94 | [0.64, 1.37] | .75 |
| Edu.: ≥Bach. (vs. ≤high school) | 0.21(0.33) | 1.23 | [0.65, 2.38] | .53 |
| Edu.: Some College (vs. ≤high school) | 0.20(0.33) | 1.22 | [0.65, 2.34] | .55 |
| Income: 100+K (vs. <50K) | 0.10(0.25) | 1.11 | [0.68, 1.80] | .68 |
| Income: 50-100K (vs. <50K) | $-0.01(0.23)$ | 0.99 | [0.63, 1.54] | .96 |
| Breach age (years) | $-0.11(0.03)$ | 0.89 | [0.83, 0.95] | < .001 |

Table 5. Logistic regression for predicting password change action in the follow-up survey. $n$=615 after excluding incomplete or not applicable responses. Cox and Snell $R^2$=0.21. Model $\chi^2(22)$=141.59, $p$<.001

*Password changes selectively made to other accounts.* For password changes regarding other accounts, almost half of the participants (48.9%) left passwords for other accounts the same. Fewer participants prioritized changing the password for other accounts using the same or similar passwords (18.5%) or for accounts they thought were important, such as bank accounts (16.3%). Only 6.1% of participants said they changed the password for every online account. The remaining 10.2% described their action for other accounts via free text, mostly mentioning that they had the habit of changing passwords regularly (e.g., *"I often change all my online passwords at least once or twice yearly"*) or they changed the password for other accounts affected by breaches after checking HIBP (e.g., *"I already use different passwords for most accounts, but I did check the list of hacked sites and I think I changed the password on one"*). Our findings are similar to results by Golla et al. [34] in

that participants developed their priorities in changing passwords for other accounts and rarely changed passwords across all accounts; however, in our study, even more participants exclusively focused on changing the password for the account affected by the breach.

*Password changes happened promptly.* Most of our participants who changed their password did it very promptly after receiving our interventions in the main survey (mean: 1.46 days; median: 1; sd: 2.24). Compared to prior work, our participants reacted to the password change prompt much faster—e.g., the mean time taken to reset the password was 26.3 days in Huh et al.'s case study of the LinkedIn breach [45], and only 13% of participants in Bhagavatula et al.'s study changed their passwords within three months of the breach announcement [8]. The differences could come from the study's methodology: we followed up with our participants two weeks since they received the breach notification, whereas in Huh et al.'s work the time gap between the breach date and data collection was several months [45]; we proactively reached out to our participants to ask about their password change, whereas Bhagavatula et al. derived their findings based on naturalistic observational data [8]. The finding implies that our interventions effectively prompted participants to follow through with their intention, and participants who forgot or did not have intention were likely to leave their password as it was without additional reminders.

*New passwords were mostly secure.* About half of our participants (50.2%) reported using a password completely unrelated to the old one they created. Some participants (32.9%) used a unique, random password generated by a password manager. Fewer participants exposed themselves to risks of password reuse attacks, either by only changing a few characters in the old password (8.8%) or by using a password that they already used for other accounts (4.7%). The remaining 3.4% self-described their new password, such as following their own password creation heuristics (e.g., *"the same password schema I use for other sites, which is known to me but generates a different password for different sites"*) and using a random password created by themselves without trying to remember it (e.g., *"I won't use that account again so I just typed in a lengthy string of numbers. If I want it again I will just recover the password"*). Compared to findings in Golla et al. [34], our participants had stronger new passwords and much fewer reused their old passwords. This is likely because our participants were creating passwords for their own accounts in real life rather than in a hypothetical scenario. The message in our coping appeal (Figure 2) could have also helped as it specifically discouraged password reuse and linked a guideline for making strong passwords.

Participants could choose multiple options to indicate their strategies for remembering the new password. Participants' strategies were diverse; the most popular options were saving the new password in the browser (27.3%), remembering the new password without writing it down or storing it digitally (25.4%), using a third-party password manager (21.0%), and writing the new password down on paper (17.9%). Less commonly, participants stored the new password in a digital file (12.2%), used a system-provided password manager (10.3%), or planned to reset the password every time they logged in rather than remember it (2.5%). Our findings align with Mayer et al. [67] and Pearman et al. [79]: participants' strategies for password management were primarily using a password manager and trying to remember it mentally.

*Difficulty in validating self-reported behaviors.* We asked participants who indicated they had changed their passwords to optionally upload a screenshot of the password reset confirmation email to verify the validity of their responses. We adapted the method from Huh et al. [45] by making the question optional but having a $1.00 bonus payment to incentivize participants and honor their time. We also explicitly reminded participants to double-check that the screenshot did not include sensitive or personal information in our instructions (Appendix A.3). Only 77 (24.1%) participants uploaded a screenshot; the rest either could not find the email (127, 39.8%) or chose not to upload

| Password Change: Yes | Count | Password Change: No | Count |
| --- | --- | --- | --- |
| to be safe | 319 | inactive use | 471 |
| bad things | 284 | no account | 321 |
| take other actions | 222 | no sensitive info | 166 |
| triggered by breach | 140 | take other actions | 120 |
| inactive use | 123 | unimportant account | 109 |

Table 6. Top reasons for changing or not changing the breached password, combing responses to Q26 ($n$=1, 386) and Q41 ($n$=1, 175).

a screenshot (115, 36.1%). In open-ended responses, participants mainly explained that they had deleted the email permanently (*"I deleted the email after receiving it, and it has probably been cleared from my Trash folder too since I try not to make my inbox too cluttered"*), they did not think it was worth the effort (*"I don't feel like searching through my email right now. Even though I would like the extra payment"*), or they were uncomfortable with the question (*"I don't feel comfortable sending my information to someone I don't personally know"*). Due to the low response rate, we did not use this question as a validation mechanism for participants' self-reported password change behaviors. While the question being optional could contribute to the low-response rate, we believed that it was a more ethical approach so that participants were not put in a position to sacrifice their data for monetary gains unwillingly. The different findings between our study and Huh et al.'s study [45] could also imply shifting norms among crowdworkers as they become more attentive and protective of their privacy [90].

## 5 QUALITATIVE RESULTS

We analyzed participants' open-ended responses regarding their rationales for changing or not changing breached passwords (Q26 and Q41), as well as their general reactions after learning about the breach (Q38). Table 6 summarizes the most prevalent themes, which we unpack below.

*Changing the password: proactive attitude.* A common theme among participants who changed their password was a proactive attitude toward staying safe and secure ($n$=319),[7] usually in the expression of *"just to be safe,"* *"to have a peace of mind,"* and *"better safe than sorry."* Such a proactive attitude could drive the action even when the participant thought the risk was limited or the account was unimportant; as one explained, *"I'm not too concerned about my MySpace info being hacked as it was such a long time ago . . . I will however change my password if that is an option just to be on the safe side."*

*Changing the password: fear of negative consequences.* Participants also mentioned various "bad things" that could occur as a result of being affected by the breach ($n$=284), which could reflect the effect of our threat appeal. One participant detailed how their personal information could be misused, *"My LiveJournal account contains fiction I wrote that I never want to lose. The knowledge that someone could delete all that work is quite perturbing."* Another participant mentioned concerns related to credential stuffing attacks, *"I want to change it because I use a lot of recycled passwords. Therefore, criminals could access other, more important accounts like e-mail accounts, bank accounts, my Amazon*

---

[7]In our findings, we report frequency counts of the most prevalent themes to help the reader understand the relative magnitudes. We consider this a valid approach as our study has a relatively large sample size, and the responses were easy to code and reliably coded. Future research that cites our qualitative findings should be careful about quoting the absolute numbers, as they were tied to a very specific setting and might not generalize well.

| Other Actions | Count |
|---|---|
| change other passwords | 171 (27.1%) |
| delete this account | 89 (14.1%) |
| try accessing account but fail | 89 (14.1%) |
| check breach records | 59 (9.3%) |
| check reused passwords | 48 (7.6%) |
| check/delete info in account | 35 (5.5%) |
| check out the breached site | 32 (5.1%) |
| review other accounts | 27 (4.3%) |

Table 7. Additional actions participants took after learning about the breach, based on responses to Q38 (*n*=632).

*account, and other online retailer accounts."* This quote also aligns our previous quantitative finding that participants who reused, or were unsure about reusing the leaked password elsewhere were more likely to form password change intention.

*Not changing the password: account inactive or low-value.* For participants who did not (intend to) change the password, the account no longer being used was the top reason (*n*=471). Relatedly, a substantial portion of participants also commented that the account did not contain much sensitive information (*n*=166) or was unimportant (*n*=109), indicating that they did not perceive the account to be high-value. As one participant reasoned, *"This account isn't important, and I'm pretty sure I haven't logged into it in almost a decade. The information contained in it would be minimal since I never really shared personal details or provided accurate information to websites for certain questions."* The unimportant comment sometimes also applies to the breached password, as one participant said, *"the password I used for it is an old and way too simple password that I don't use for my important accounts. I have used that password for some accounts like free online games but that is it."*

*Not changing the password: no account with the breached site.* Participants also commented on the practical constraints that made password change impossible or difficult. For instance, 321 participants believed that they did not have an account with the breached site, as they did not recognize the site's name, recognized the site but did not remember making an account, or the account was already deleted. Without an account, the advice of changing the breached password for that account becomes unrealistic, as one participant wrote, *"I do not have a Quidd account so there is no password to change."* Another 86 participants confirmed that their account indeed no longer existed, as they tried to log into the account but failed, because the site did not recognize the email address provided, the site was down, or they never received the password reset email. Data brokers might also contribute to the problem, as one participant speculated, *"When I tried to reset my password, the email never came . . . Maybe these sites had bought my information somehow from some other place, and therefore were able to obtain a username/email and password from me despite me never opening an account with them directly."*

*Actions taken other than changing the password.* As "take other actions" emerged as a common theme, regardless of whether the participant changed the breached password, we summarize what these actions are in Table 7, derived from responses to Q38. When changing the password for other online accounts (*n*=171), some participants made the change to all accounts while others prioritized important accounts, e.g., *"I changed my Gmail password since that is the only account I'm particularly worried about."* To determine which accounts were at higher risk, 59 participants obtained a more

comprehensive list of breach records to guide their password changes. Another 48 participants reviewed their existing passwords to identify those that were reused and should be changed first.

Some other actions taken by participants were unrelated to passwords. For instance, 89 participants deleting their account on the breached site, as one participant recounted, *"After the previous survey, I did change my password. Later that day, I decided to just delete my account. I never really did use that site anyway, and it just got me thinking that I really didn't need to have any info at all on it."* Expecting that they may need to use the account in the future, another 35 participants checked content in the account to ensure there was no sensitive information. As one participant detailed their experience, *"I immediately went to my LiveJournal account, where I changed my password and the email address associated with the account. I also confirmed that all posts which contained potentially identifying information were either deleted or set to private."* Other actions taken include searching for more information about the breached site ($n$=32) and reviewing and sometimes deleting other inactive accounts ($n$=27).

## 6 DISCUSSION

Our experiment compared the effectiveness of interventions that incorporate a threat appeal, a coping appeal, or both, against a control condition. We focused on the impacts of these interventions on participants' intended and actual behaviors around password changes after data breaches. Compared to the control condition, a threat appeal alone significantly increased participants' intention to change their passwords, and threat and coping appeals combined significantly increased participants' password change behavior. The effect size was small in both comparisons, and no significant differences were found between the three treatment conditions. Participants further described issues they encountered when trying to change their breached password and alternative actions they took. We next discuss our study's limitations, then summarize how our findings contribute new knowledge to PMT literature and their implications for designing compromised credential notifications.

### 6.1 Limitations

Our work has multiple limitations. First, we situated our interventions in breach records curated by HIBP. While HIBP is a reputable source and has been integrated into other services such as Firefox Monitor and 1Password, the database mainly consists of username and password breaches since it is built on scans of account credential dumps. Other types of personally identifiable information, such as social security numbers and medical records, rarely appear in HIBP's database, but they do appear in other databases of breach records [47]. Some of our findings could be different if participants were presented with breaches that exposed more intimate details of themselves. Because publicly available APIs for accessing breach records (like the one provided by HIBP) are still rare, future research could build a tool to curate breach records from multiple sources or partner with companies and/or non-profit organizations to replicate our results.

Second, some of the limitations relate to our sampling of participants. We conducted our experiment only with participants recruited in the US. We relied on Prolific for recruitment, which led to the exclusion of less tech-savvy participants such as those without Internet access. These recruitment criteria limit our findings' generalizability beyond the US and more tech-savvy consumers. Thus, they introduce opportunities for future research to replicate our study in different locations with different legal and consumer protection frameworks around data breaches.

Third, our evaluation relies on participants' self-reported data. While self-reported data is subject to issues such as recall and social desirability biases, prior research has shown self-reported data varies consistently and systematically with measured data in security user studies when the experimental manipulations have non-trivial variations [84], which is the case in our study. Our

attempt to validate participants' self-reported action via screenshots was unsuccessful due to the low response rate for this optional question. Future research could implement our experimental protocol on real-world measurement data and compare them to self-reported data to identify whether a significant gap exists between the two.

Lastly, a minority of our survey questions were not perfect measures for their intended constructs. As discussed in Section 4.4, we had to exclude responses about the account's information type due to the absence of a "none of the above" option. Additionally, our questions about the account's age, the purpose of use, and perceived importance might not capture all nuances as participants' account usage evolves. Future work could consider specifying the timing of account-checking (e.g., ask "When was the last time you checked the account?" rather than "How often do you check the account?") and using Likert scales rather than single Likert items for concepts such as perceived account importance to more accurately characterize users' diverse account usage behaviors.

## 6.2 Contributions to the PMT Literature

*Comparing our findings to existing PMT literature.* Our findings add to the ongoing discussion in PMT research about whether threat or coping appraisal plays a more prominent role in individuals' formation of protection motivation. Our findings highlight an interesting pattern: compared to the control condition, the threat appeal alone performed significantly better at raising password change intention, but the combination of threat and coping appeals performed significantly better at driving actual password changes.

Comparing our findings with PMT's application in other security contexts, our findings confirm that it usually requires both threat and coping appeals to drive action, as has been shown in the cases of adopting secure mobile payments [99] and Tor browser adoption [100]. Comparing our findings to those of van Bavel et al. [114], who similarly differentiated threat from coping appeals, we observe a different pattern, as in their study the coping appeal was more effective than the threat appeal in nudging participants toward secure online purchases [114]. The different finding might be due to the simulated environment in their experiment: participants would not have experienced the errors and usability issues that can occur with real-world online accounts, which could impact their coping behaviors subsequently.

Comparing our findings with PMT's application in other contexts beyond security and privacy, we find that the context featured might explain the different findings. In two meta-analyses of the PMT literature in the health domain, the coping appraisal components were found to have greater predictive validity than the threat appraisal components for both behavioral intentions and actual behaviors [29, 73]. Importantly, for health-education interventions, the threat that the protective behavior seeks to address—whether it is stroke, heart disease, or cancer—is likely to be obvious and salient to most people. By comparison, the threat of a breached password may be more nebulous. Nevertheless, highlighting this threat, especially as we walked participants through how credential stuffing attacks work, could have made a bigger difference. Our context also introduces unique considerations for the coping behavior. While a health-related behavior (e.g., breast self-examination, smoking cessation, or adopting a healthy diet) is applicable to most people, this is not the case for changing a breached password. As evidenced by our qualitative results, a non-trivial portion of our participants did not have an account with the breached site or encountered issues as they tried to change the breached password. These are unfortunate scenarios that cannot be addressed by a coping appeal, no matter how effective it is.

*The limitations of applying PMT to motivate password changes.* Our results shed light on the limitations of PMT by identifying other factors that explain variances in participants' password change behavior and the hurdles participants experience in changing their passwords. An example

of such factors is attitude. Prior work has showcased how attitude influenced security intention and behavior [48, 96, 114], yet 'attitude' is a broad term that can apply to many subjects, from the recommended action to risks in general. Our work highlights the importance of security attitudes more precisely: from the regression results, SA-6 was a significant predictor in both the intention and action models; from the qualitative findings, "to be safe" is a prevalent theme.

Another contextual factor that impacts password change behaviors is the breach's timing. The regression results suggest that participants were less likely to change the account password for breaches that happened a long time ago. Our qualitative analysis further provides insights into why. For example, one participant reasoned that so much time has passed that the breached information was no longer relevant, *"The breach happened so long ago that I'm sure that password is not being used anywhere else for my accounts online. Along with the other compromised information, it's no longer the same, except my name which is common knowledge and published on the internet anyways."*

Moreover, while PMT exclusively focuses on appraisals and hurdles in human cognitive processing, what needs to be considered in our study's particular context is systemic issues regarding the password ecosystem. For instance, forgetting or not knowing an old password was a common theme for inaction, yet when an average American user has over 150 online accounts that require a password [21], keeping track of different passwords for every single account is fundamentally challenging, especially for those who have not developed a password management system [28, 78]. In attempting to change their passwords, participants encountered some issues that were technically out of their control, e.g., the site told them there was no account that matched the provided email address, they struggled to find the password reset button, or they struggled to identify which account to change when the breached company owned many sites that the account could belong to. Some of these issues might be unintended consequences of the site's attempt to comply with privacy regulations, e.g., when the site deletes inactive accounts to meet GDPR's data minimization requirement [26]. Others were akin to the usability issues of privacy controls [38, 39], and could even be viewed as dark patterns that sites deploy to coerce users into staying in business with them [74].

## 6.3 Practical Implications

Our interventions have several promising avenues for deployment. Breach notifications are already mandated by many data breach disclosure laws around the world [87, 127], mostly via mailed letters but also increasingly via digital channels such as emails. For password breaches in particular, compromised credential checking had been adopted as a feature in mainstream browsers (e.g., Google Chrome and Microsoft Edge) [61, 81] as well as in password managers (e.g., 1Password and LastPass) [31, 95]. Another way to notify users is during the next time they access a particular online account that has been affected by breaches, as this represents a natural moment for them to interact with the breached password. Our findings help inform best practices for designing notifications in these settings, as we discuss below.

*Highlight threats, but with caution.* Prior work has highlighted misunderstandings users may have in assessing the risks of data breaches and password reuse [8, 34, 69, 128] as well as proposed ideas to address them. For example, Golla et al. [34] advocated that the notification should encourage users to change similar passwords on other accounts and thoroughly explain why doing so mitigates password reuse attacks. Huang et al. [44] drew specific recommendations for Chrome's compromised credential notification, suggesting more explanations about why it is necessary to change the breached password and what risks the user may face if they do not change their passwords. Our study directly tested Huang et al.'s proposed idea, and our findings confirm that a threat appeal is useful to raise users' intention to change their breached credentials.

Nevertheless, the threat appeal alone performed only marginally better than the control condition at raising password change intentions, if judged by the effect size. As such, we caution that service providers should consider the returns and potential unintended consequences of overly emphasizing threats. One needs to consider whether iterating, implementing, and evaluating the threat appeal is worth the effort if a plain notification with less text can achieve the same purpose most of the time. To avoid overwhelming users, prior work has recommended providing information in a layered form [17, 25, 44], and we incorporated this format in our visual displays of the nudging text. Unfortunately, we cannot know if the layered approach truly results in an improvement since we did not conduct A/B testing on this feature. This could be an opportunity for future research, especially considering that the specific layer designs will likely differ across products and interfaces.

Furthermore, there might be inevitable tensions between highlighting threats and making the notification trauma-informed. Security incidents like data breaches can trigger traumatic and stressful experiences [14]. Prior work has highlighted that a threat appeal, when being too strong, could be counter-productive, especially for those already in a vulnerable state: they may engage in risk denial or simply refuse to engage with the fearful message as a self-protective mechanism because the threat makes them feel uncomfortable [88]. Our participants appreciated our interventions for informing them of the breach, and no one explicitly commented on the message being too triggering. Yet some participants recounted how busy they were or how they got distracted by other things, suggesting that an inappropriately designed threat appeal could generate unnecessary burdens or anxiety. This is where a coping appeal could come into play and ease potential stress reactions triggered by the threat appeal, such as by telling the user that they could pick a later time to deal with the issue and asking them if they want a reminder for this [100].

*Communicate data flows to mitigate distrust.* Trust issues can prevent users from adopting password managers or adhering to security advice. In Huang et al.'s study [44], many participants' concerns were related to Google, as they assumed that Google checks their non-saved credentials, or they worried about Google taking control over their own data. By contrast, none of our participants expressed concerns about HIBP, which we explicitly highlighted as the source of the breach records, perhaps because of the service's non-profit nature. Interestingly, our participants' concerns mostly centered around the breached site, e.g., when they were unfamiliar with the site's name or when they were concerned about additional data leaks that could happen as they sought to recover their account.

These findings highlight the necessity of providing more transparency to mitigate potential questions, distrust, and misunderstandings among users, but how to do so well remains a key challenge. Prior work has recommended that browsers and password managers that send compromised credential notifications should explain how the product detects leaked or reused passwords [44] and, on a higher level, what measures the company takes to protect users' data [83]. Service providers are already doing this to some extent in their messaging (e.g., see "Privacy is at the heart of our design" in Google's blog post about its password checkup feature) [81]. Still, the deeper issue is users' lack of awareness of and trust in encryption [22, 126], which will likely cause comprehension problems for such messaging. Helping users build trust with the breached site is more tricky, as users have reasonable doubts about the site for leaking or exposing their data in the first place. Proactively reaching out to affected users might help, as our participants expressed that they would rather learn about and deal with the breach rather than stay uninformed. For instance, one participant said, *"I do not remember receiving any notice from Poshmark. They can't even spend the resources to notify us."* If the user trusts the site enough to check it out, there could be additional explanations of when and how their account was created (if it still exists) or why their account no longer exists.

*Standardizing and semi-automating the password change experience.* The various challenges our participants experienced in attempting to change their passwords highlight larger problems with the password ecosystem. As much as we tried to predict edge cases in developing our coping appeal, our findings reflect that the real-world situation is far more complex. Participants could encounter all kinds of scenarios in which things could go wrong. It then becomes difficult to predict all scenarios and enumerate corresponding solutions in a concise coping appeal.

Our findings reflect that the experience of changing a password could be drastically different from site to site. However, it should not be this way, and we see the need for standardizing the password change processes by providing more industry guidelines or pushing for stronger regulations. For example, the California Consumer Privacy Act (CCPA) requires businesses to include a "Do Not Sell My Personal Information" link on their website that allows consumers to submit an opt-out request (if the business sells personal information) [76]. We imagine similar efforts could be made to standardize where websites should provide the account login fields as well as information regarding how to change the account password. The CAN-SPAM Act in the US requires that for commercial messages, businesses should honor consumers' opt-out requests within ten business days [103]. Similarly, we see opportunities for standardizing the turnaround time for sending password reset confirmations, given that one of the hurdles our participants reported was struggling to find the password reset email.

Beyond standardization, we see opportunities for partially automating the password change experience. For instance, for someone who already adopts a password manager, the password manager could provide a feature that allows the user to scan through every saved login credential and determines whether it still works for the corresponding site.

*Opportunities and challenges for providing personalized advice.* Our findings reveal the cost-benefit analysis behind participants' decision to change the breached password. The action was reasonable for someone who used the account extensively and felt motivated to protect it from potential compromises. However, participants who did not care about the account tended to delete the account instead, and participants who were already using strong and unique passwords for different accounts had valid reasons for not changing the password since their risk levels were minimal.

Our findings call for a deeper reflection on whether changing the breached password should be the nudging goal for everyone given the diverse risk levels and preferences among individuals. We see the promises of personalized advice to help consumers better assess whether password changes are needed in their particular situations. For instance, existing password managers such as 1Password and LastPass are already providing dashboards and scores that help users evaluate overall password strength and the extent of password reuse [23, 60]. Going beyond these features, password managers could provide personalized and data-driven recommendations on which account(s) to prioritize (such as banking and shopping sites that are more likely to contain financial information) in cleaning up old or weak passwords. In addition, advice on which actions to take should ideally be tailored to the specific types of compromised information. Breaches that involve more sensitive or unique data types, such as social security numbers or medical records, might require more serious measures. Existing advice for what to do after data breaches mostly enumerates different actions depending on the different breached data types [52]. A more efficient way could be presenting personalized advice in the order of priority. The interactive resource provided by the US Federal Trade Commission [102] is a good step toward this direction, although the extent of personalization there is still quite limited.

While we see exciting opportunities offered by personalizing post-breach coping advice, we should not ignore challenges associated with personalization. Too much automation, while reducing users' burden, could reduce their sense of agency [15]. The personalized advice might be inaccurate

or irrelevant, which may further cause trust issues or annoy users. When the advice is about password changes in particular, the personalization will likely need to be offered via password managers, which have an increasing yet still small user base [67]. The dependence on password managers might also exclude specific populations like older adults, who are known to have more trust issues with cloud storage of passwords [82]. The questions then become: how do we find a balance between making personalized advice useful versus learning too much about users' preferences to the extent of causing privacy concerns? How do we make personalized advice accessible to everyone and truly reflect users' diverse needs and preferences?

## ACKNOWLEDGMENTS

## REFERENCES

[1] Svetlana Abramova and Rainer Böhme. Anatomy of a high-profile data breach: Dissecting the aftermath of a crypto-wallet case. In *USENIX Security Symposium*, pages 715–732, Anaheim, CA, USA, August 2023. USENIX. https://www.usenix.org/system/files/usenixsecurity23-abramova.pdf.

[2] Icek Ajzen. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991. doi:10.1016/0749-5978(91)90020-T.

[3] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 31–46, Baltimore, MD, USA, August 2018. USENIX. https://www.usenix.org/system/files/conference/soups2018/soups2018-qahtani.pdf.

[4] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Symposium on Usable Privacy and Security*, pages 49–63, Santa Clara, CA, USA, July 2017. USENIX. https://www.usenix.org/system/files/conference/soups2017/soups2017-albayram.pdf.

[5] Nora Alkaldi and Karen Renaud. Why Do People Adopt, or Reject, Smartphone Password Managers? In *European Workshop on Usable Security*, pages 5:1–5:14, Darmstadt, Germany, July 2016. Internet Society. doi:10.14722/eurousec.2016.23011.

[6] Nora Alkaldi, Karen Renaud, and Lewis Mackenzie. Encouraging password manager adoption by meeting adopter self-determination needs. In *Hawaii International Conference on System Sciences*, pages 4824–4833, Kauai, HI, USA, January 2019. ScholarSpace. doi:10.24251/HICSS.2019.582.

[7] Catherine L Anderson and Ritu Agarwal. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3):613–643, 2010. doi:10.2307/25750694.

[8] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. (How) Do People Change Their Passwords After a Breach? In *Workshop on Technology and Consumer Protection*, pages 8:1–8:8, Virtual Conference, May 2020. IEEE. https://www.ieee-security.org/TC/SPW2020/ConPro/papers/bhagavatula-conpro20.pdf.

[9] Jan Boehmer, Robert LaRose, Nora Rifon, Saleem Alhabash, and Shelia Cotten. Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, 34(10):1022–1035, 2015. doi:10.1080/0144929X.2015.1028448.

[10] Scott R Boss, Dennis F Galletta, Paul Benjamin Lowry, Gregory D Moody, and Peter Polak. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4):837–864, 2015. doi:10.25300/MISQ/2015/39.4.5.

[11] AJ Burns, Clay Posey, Tom L Roberts, and Paul Benjamin Lowry. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68:190–209, 2017. doi:10.1016/j.chb.2016.11.018.

[12] Xavier De Carné De Carnavalet and Mohammad Mannan. A large-scale evaluation of high-impact password strength meters. *ACM Transactions on Information and System Security*, 18(1):1:1–1:32, 2015. doi:10.1145/2739044.

[13] Henian Chen, Patricia Cohen, and Sophie Chen. How big is a big odds ratio? interpreting the magnitudes of odds ratios in epidemiological studies. *Communications in Statistics—simulation and Computation*, 39(4):860–864, 2010. doi:10.1080/03610911003650383.

[14] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. Trauma-informed computing: Towards safer technology experiences for all. In *ACM Conference on Human Factors in Computing Systems*, pages 544:1–544:20, New Orleans, LA, USA, April 2022. ACM. doi:10.1145/3491102.3517475.

[15] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *ACM Conference on Human Factors in Computing Systems*, pages 262:1–262:13, Honolulu, HI, USA, 2020. ACM. doi:10.1145/3313831.3376389.

[16] Lorrie Cranor. Time to rethink mandatory password changes, March 2016. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2016/03/time-rethink-mandatory-password-changes, accessed on: August 13, 2024.

[17] Lorrie Faith Cranor. Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law*, 10(2):273–308, 2012.

[18] Robert E Crossler, James H Long, Tina M Loraas, and Brad S Trinkle. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems*, 28(1):209–226, 2014. doi:10.2308/isys-50704.

[19] Cybersecurity & Infrastructure Security Agency. Security Tip (ST04-002) Choosing and Protecting Passwords, May 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-002, accessed on: August 13, 2024.

[20] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security*, pages 26:1–26:15, San Diego, CA, USA, February 2014. Internet Society. doi:10.14722/NDSS.2014.23357.

[21] Dashlane. World Password Day: How to Improve Your Passwords, May 2018. https://blog.dashlane.com/world-password-day/, accessed on: August 13, 2024.

[22] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In *European Symposium on Security and Privacy*, pages 401–415, Stockholm, Sweden, June 2019. IEEE. doi:10.1109/EuroSP.2019.00037.

[23] Kerry DeVito. How to improve your Watchtower score in 1Password, May 2022. https://blog.1password.com/improve-watchtower-score-1password/, accessed on: August 13, 2024.

[24] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *ACM Conference on Human Factors in Computing Systems*, pages 2379–2388, Paris, France, April 2013. ACM. doi:10.1145/2470654.2481329.

[25] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *ACM Conference on Human Factors in Computing Systems*, pages 534:1–534:12, Glasgow, Scotland, UK, April 2019. ACM. doi:10.1145/3290605.3300764.

[26] The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27. April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), May 2016. http://data.europa.eu/eli/reg/2016/679/oj, accessed on: August 13, 2024.

[27] Cori Faklaris, Laura A Dabbish, and Jason I Hong. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Symposium on Usable Privacy and Security*, pages 61–77, Santa Clara, CA, USA, August 2019. USENIX. https://www.usenix.org/system/files/soups2019-faklaris.pdf.

[28] Dinei Florêncio and Cormac Herley. A Large-scale Study of Web Password Habits. In *The World Wide Web Conference*, pages 657–666, Banff, Alberta, Canada, May 2007. ACM. doi:10.1145/1242572.1242661.

[29] Donna L Floyd, Steven Prentice-Dunn, and Ronald W Rogers. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2):407–429, 2000. doi:10.1111/j.1559-1816.2000.tb02323.x.

[30] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. In *Symposium on Usable Privacy and Security*, pages 97–111, Denver, CO, USA, June 2016. USENIX. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-forget.pdf.

[31] Rose de Fremery. Breaking the Cycle of Password Reuse, September 2021. https://blog.lastpass.com/2021/09/breaking-the-cycle-of-password-reuse/, accessed on: August 13, 2024.

[32] Shirley Gaw and Edward W. Felten. Password Management Strategies for Online Accounts. In *Symposium on Usable Privacy and Security*, pages 44–55, Pittsburgh, PA, USA, July 2006. ACM. doi:10.1145/1143120.1143127.

[33] A Ian Glendon and Britta L Walker. Can anti-speeding messages based on protection motivation theory influence reported speeding intentions? *Accident Analysis & Prevention*, 57:67–79, 2013. doi:10.1016/j.aap.2013.04.004.

[34] Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, and Blase Ur. "What was that site doing with my Facebook password?" Designing Password-Reuse Notifications. In *ACM Conference on Computer and Communications Security*, pages 1549–1566, Toronto, Ontario, Canada, October 2018. ACM.

doi:10.1145/3243734.3243767.

[35] Peter M Gollwitzer. Implementation intentions: strong effects of simple plans. *American Psychologist*, 54(7):493–503, 1999. doi:10.1037/0003-066X.54.7.493.

[36] Paul A Grassi, Michael E Garcia, and James L Fenton. Digital Identity Guidelines – NIST Special Publication 800-63-3, June 2017. doi:10.6028/NIST.SP.800-63-3.

[37] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. User Behaviors and Attitudes Under Password Expiration Policies. In *Symposium on Usable Privacy and Security*, pages 13–30, Baltimore, MD, USA, August 2018. USENIX. https://www.usenix.org/system/files/conference/soups2018/soups2018-habib-password.pdf.

[38] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *ACM Conference on Human Factors in Computing Systems*, pages 384:1–384:12, Honolulu, HI, USA, April 2020. ACM. doi:10.1145/3313831.3376511.

[39] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An Empirical Analysis of Data Deletion and Opt-out Choices on 150 Websites. In *Symposium on Usable Privacy and Security*, pages 387–406, Santa Clara, CA, USA, August 2019. USENIX. https://www.usenix.org/system/files/soups2019-habib.pdf.

[40] Bartlomiej Hanus and Yu "Andy" Wu. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, 33(1):2–16, 2016. doi:10.1080/10580530.2015.1117842.

[41] Benjamin Harkin, Thomas L Webb, Betty PI Chang, Andrew Prestwich, Mark Conner, Ian Kellar, Yael Benn, and Paschal Sheeran. Does monitoring goal progress promote goal attainment? a meta-analysis of the experimental evidence. *Psychological Bulletin*, 142(2):198–229, 2016. doi:10.1037/bul0000025.

[42] Tejaswini Herath and H Raghav Rao. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2):106–125, 2009. doi:10.1057/ejis.2009.6.

[43] Joanne Hinds, Emma J Williams, and Adam N Joinson. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143:102498, 2020. doi:10.1016/j.ijhcs.2020.102498.

[44] Yue Huang, Borke Obada-Obieh, and Konstantin Beznosov. Users' Perceptions of Chrome Compromised Credential Notification. In *Symposium on Usable Privacy and Security*, pages 155–174, Boston, MA, USA, August 2022. USENIX. https://www.usenix.org/system/files/soups2022-huang_1.pdf.

[45] Jun Ho Huh, Hyoungshick Kim, Swathi S.V.P. Rayala, Rakesh B. Bobba, and Konstantin Beznosov. I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails. In *ACM Conference on Human Factors in Computing Systems*, pages 387–391, Denver, CO, USA, May 2017. ACM. doi:10.1145/3025453.3025788.

[46] Troy Hunt. Pwned websites, August 2022. https://haveibeenpwned.com/PwnedWebsites, accessed on: August 13, 2024.

[47] Identity Theft Resource Center. Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises, January 2022. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/, accessed on: August 13, 2024.

[48] Princely Ifinedo. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1):83–95, 2012. doi:10.1016/j.cose.2011.10.007.

[49] Nancy K Janz and Marshall H Becker. The health belief model: A decade later. *Health Education Quarterly*, 11(1):1–47, 1984. doi:10.1177/109019818401100101.

[50] Jeffrey Jenkins, Alexandra Durcikova, and Jay F Nunamaker Jr. Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship. *Journal of the Association for Information Systems*, 22(1):246–272, 2021. doi:10.17705/1jais.00660.

[51] Jeffrey L Jenkins, Mark Grimes, Jeffrey Gainer Proudfoot, and Paul Benjamin Lowry. Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, 20(2):196–213, 2014. doi:10.1080/02681102.2013.814040.

[52] Alison Grace Johansen. What to do after 5 types of data breaches, October 2021. https://us.norton.com/blog/emerging-threats/what-to-do-after-a-data-breach, accessed on: August 13, 2024.

[53] Allen C Johnston and Merrill Warkentin. Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3):549–566, 2010. doi:10.2307/25750691.

[54] Allen C Johnston, Merrill Warkentin, and Mikko Siponen. An enhanced fear appeal rhetorical framework. *MIS Quarterly*, 39(1):113–134, 2015. doi:10.25300/misq/2015/39.1.06.

[55] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data. In *Symposium on Usable Privacy and Security*, pages 217–234, Baltimore, MD, USA, August 2018. USENIX. https://www.usenix.org/system/files/conference/soups2018/soups2018-karunakaran.pdf.

[56] Lindall R Kidd, Georgia E Garrard, Sarah A Bekessy, Morena Mills, Adrian R Camilleri, Fiona Fidler, Kelly S Fielding, Ascelin Gordon, Emily A Gregg, Alexander M Kusmanoff, Winnifred Louis, Katie Moon, Jenny Robinson, Matthew J Selinske, Danielle Shanahan, and Vanessa Adams. Messaging matters: A systematic review of the conservation messaging literature. *Biological Conservation*, 236:92–99, 2019. doi:10.1016/j.biocon.2019.05.020.

[57] Emily J Kothe, Mathew Ling, Madelon North, Anna Klas, Barbara A Mullan, and Lisa Novoradovskaya. Protection motivation theory and pro-environmental behaviour: A systematic mapping review. *Australian Journal of Psychology*, 71(4):411–432, 2019. doi:10.1111/ajpy.12271.

[58] Isadora Krsek, Kimi Wenzel, Sauvik Das, Jason I Hong, and Laura Dabbish. To self-persuade or be persuaded: Examining interventions for users' privacy setting selection. In *ACM Conference on Human Factors in Computing Systems*, pages 623:1–623:17, New Orleans, LA, USA, April 2022. ACM. doi:10.1145/3491102.3502009.

[59] Robert LaRose, Nora J Rifon, and Richard Enbody. Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3):71–76, 2008. doi:10.1145/1325555.1325569.

[60] LastPass. Digital Security Dashboard, January 2022. https://www.lastpass.com/features/security-dashboard, accessed on: August 13, 2024.

[61] Kristin Lauter, Sreekanth Kannepalli, Kim Laine, and Radames Cruz Moreno. Password Monitor: Safeguarding passwords in Microsoft Edge, January 2021. https://www.microsoft.com/en-us/research/blog/password-monitor-safeguarding-passwords-in-microsoft-edge/, accessed on: August 13, 2024.

[62] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, San Francisco, CA, USA, 2017.

[63] Richard S Lazarus and Susan Folkman. *Stress, Appraisal, and Coping.* Springer, New York, NY, USA, 1984.

[64] Doohwang Lee, Robert Larose, and Nora Rifon. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5):445–454, 2008. doi:10.1080/01449290600879344.

[65] James E Maddux and Ronald W Rogers. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, 19(5):469–479, 1983. doi:10.1016/0022-1031(83)90023-9.

[66] Peter Mayer, Alexandra Kunz, and Melanie Volkamer. Reliable behavioural factors in the information security context. In *International Conference on Availability, Reliability and Security*, pages 9:1–9:10, Reggio Calabria, Italy, August 2017. ACM. doi:10.1145/3098954.3098986.

[67] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. Why Users (Don't) Use Password Managers at a Large Educational Institution. In *USENIX Security Symposium*, pages 1849–1866, Boston, MA, USA, August 2022. USENIX. https://www.usenix.org/system/files/sec22-mayer.pdf.

[68] Peter Mayer, Yixin Zou, Byron M Lowens, Hunter A Dyer, Khue Le, Florian Schaub, and Adam J Aviv. Awareness, Intention,(In) Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction*, 30(5):77:1–77:53, 2023. doi:10.1145/3589958.

[69] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *USENIX Security Symposium*, pages 393–410, Virtual Conference, August 2021. USENIX. https://www.usenix.org/system/files/sec21fall-mayer.pdf.

[70] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur. Measuring Password Guessability for an Entire University. In *ACM Conference on Computer and Communications Security*, pages 173–186, Berlin, Germany, November 2013. ACM. doi:10.1145/2508859.2516726.

[71] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):72:1–72:23, 2019. doi:10.1145/3359174.

[72] B Dawn Medlin and Joseph A Cazier. An Empirical Investigation: Health Care Employee Passwords and Their Crack Times in Relationship to HIPAA Security Standards. *International Journal of Healthcare Information Systems and Informatics*, 2(3):39–48, 2007. doi:10.4018/jhisi.2007070104.

[73] Sarah Milne, Paschal Sheeran, and Sheina Orbell. Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(1):106–143, 2006. doi:10.1111/j.1559-1816.2000.tb02308.x.

[74] Deirdre K Mulligan, Priscilla M Regan, and Jennifer King. The fertile dark matter of privacy takes on the dark patterns of surveillance. *Journal of Consumer Psychology*, 30(4):767–773, 2020. doi:10.1002/jcpy.1190.

[75] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie Calvin Xu. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4):815–825, 2009. doi:10.1016/j.dss.2008.11.010.

[76] Office of the California Attorney General. California Consumer Privacy Act (CCPA): Final Text of Proposed Regulations, March 2020. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf, accessed on: August 13, 2024.

[77] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. What Happens After You Are Pwnd: Understanding the Use of Leaked Webmail Credentials in the Wild. In *Internet Measurement Conference*, pages 65–79, Santa Monica, CA, USA, November 2016. ACM. doi:10.1145/2987443.2987475.

[78] 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 *Conference on Computer and Communications Security*, pages 295–310, Dallas, TX, USA, October 2017. ACM. doi:10.1145/3133956.3133973.

[79] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security*, pages 319–338, Santa Clara, CA, USA, August 2019. USENIX. https://www.usenix.org/system/files/soups2019-pearman.pdf.

[80] 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. doi:10.1016/j.chb.2020.106347.

[81] Jennifer Pullman, Kurt Thomas, and Elie Bursztein. Protect your accounts from data breaches with Password Checkup, February 2019. https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html, accessed on: August 13, 2024.

[82] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J Aviv. Why older adults (don't) use password managers. In *USENIX Security Symposium*, pages 73–90, Virtual Conference, 2021. USENIX. https://www.usenix.org/system/files/sec21-ray.pdf.

[83] Elissa M. Redmiles. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *IEEE Symposium on Security and Privacy*, pages 920–934, San Francisco, CA, USA, May 2019. IEEE. doi:10.1109/SP.2019.00059.

[84] Elissa M. Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L. Mazurek. Asking for a Friend: Evaluating Response Biases in Security User Studies. In *ACM Conference on Computer and Communications Security*, pages 1238–1255, Toronto, Ontario, Canada, October 2018. ACM. doi:10.1145/3243734.3243740.

[85] Ronald W Rogers. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1):93–114, 1975. doi:10.1080/00223980.1975.9915803.

[86] Ronald W Rogers. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, pages 153–176, 1983.

[87] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, 30(2):256–286, 2011. doi:10.1002/pam.20567.

[88] Robert AC Ruiter, Loes TE Kessels, Gjalt-Jorn Y Peters, and Gerjo Kok. Sixty years of fear appeal research: Current state of the evidence. *International journal of psychology*, 49(2):63–70, 2014. doi:10.1002/ijop.12042.

[89] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. Sage, Thousand Oaks, CA, USA, 2015.

[90] Shruti Sannon, Billie Sun, and Dan Cosley. Privacy, surveillance, and power in the gig economy. In *ACM Conference on Human Factors in Computing Systems*, pages 619:1–619:15, New Orleans, LA, USA, April 2022. ACM. doi:10.1145/3491102.3502083.

[91] Richard Shay, Iulia Ion, Robert W. Reeder, and Sunny Consolvo. "My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking. In *ACM Conference on Human Factors in Computing Systems*, pages 2657–2666, Toronto, Ontario, Canada, April 2014. ACM. doi:10.1145/2556288.2557330.

[92] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security*, 18(4):13:1–13:34, 2016. doi:10.1145/2891411.

[93] Paschal Sheeran and Thomas L Webb. The intention–behavior gap. *Social and Personality Psychology Compass*, 10(9):503–518, 2016. doi:10.1111/spc3.12265.

[94] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, 48:199–207, 2015. doi:10.1016/j.chb.2015.01.046.

[95] Jeff Shiner. Finding compromised passwords with 1Password, August 2018. https://blog.1password.com/finding-pwned-passwords-with-1password/, accessed on: August 13, 2024.

[96] Mikko Siponen, M Adam Mahmood, and Seppo Pahnila. Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2):217–224, 2014. doi:10.1016/j.im.2013.08.006.

[97] Daniel J Solove and Woodrow Hartzog. *Breached!: Why Data Security Law Fails and How to Improve it*. Oxford University Press, Oxford, UK, 2022.

[98] Elizabeth Stobert and Robert Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *Symposium on Usable Privacy and Security*, pages 243–255, Menlo Park, CA, USA, July 2014. USENIX. https://www.usenix.org/system/files/conference/soups2014/soups14-paper-stobert.pdf.

[99] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. From intent to action: Nudging users towards secure mobile payments. In *Symposium on Usable Privacy and Security*, pages 379–415, Virtual Conference, August 2020. USENIX. https://www.usenix.org/system/files/soups2020-story.pdf.

[100] Peter Story, Daniel Smullen, Rex Chen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Increasing Adoption of Tor Browser Using Informational and Planning Nudges. *Proceedings on Privacy Enhancing Technologies*, 2:152–183, 2022. doi:10.2478/popets-2022-0040.

[101] Richard H Thaler and Cass R Sunstein. *Nudge: The final edition*. Yale University Press, 2021.

[102] The Federal Trade Commission. When information is lost or exposed, January 2020. https://www.identitytheft.gov/databreach, accessed on: August 13, 2024.

[103] The Federal Trade Commission. CAN-SPAM Act: A Compliance Guide for Business, August 2023. https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business, accessed on: August 13, 2024.

[104] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, Daniel Margolis, Vern Paxson, and Elie Bursztein. Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials. In *ACM Conference on Computer and Communications Security*, pages 1421–1434, Dallas, TX, USA, October 2017. ACM. doi:10.1145/3133956.3134067.

[105] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, and Elie Bursztein. Protecting Accounts from Credential Stuffing with Password Breach Alerting. In *USENIX Security Symposium*, pages 1556–1571, Santa Clara, CA, USA, August 2019. USENIX. https://www.usenix.org/system/files/sec19-thomas.pdf.

[106] United Kingdom National Cybersecurity Center. Password administration for system owners, January 2018. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach, accessed on: August 13, 2024.

[107] United States Census Bureau. Age and Sex Tables, January 2022. https://www.census.gov/topics/population/age-and-sex/data/tables.2019.List_897222059.html, accessed on: August 13, 2024.

[108] United States Census Bureau. Census Bureau Releases New Educational Attainment Data, January 2022. https://www.census.gov/newsroom/press-releases/2022/educational-attainment.html, accessed on: August 13, 2024.

[109] United States Census Bureau. Selected Characteristics of Households by Total Money Income, January 2022. https://www.census.gov/data/tables/time-series/demo/income-poverty/cps-hinc/hinc-01.html, accessed on: August 13, 2024.

[110] United States Census Bureau. U.S. Census Bureau QuickFacts, January 2022. https://www.census.gov/quickfacts/fact/table/US/LFE046220, accessed on: August 13, 2024.

[111] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do Users' Perceptions of Password Security Match Reality? In *ACM Conference on Human Factors in Computing Systems*, pages 3748–3760, San Jose, CA, USA, May 2016. ACM. doi:10.1145/2858036.2858546.

[112] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium*, pages 65–80, Bellevue, WA, USA, August 2012. USENIX. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final209.pdf.

[113] 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 *Symposium on Usable Privacy and Security*, pages 123–140, Ottawa, Ontario, Canada, July 2015. USENIX. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ur.pdf.

[114] René van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123:29–39, 2019. doi:10.1016/j.ijhcs.2018.11.003.

[115] Anthony Vance, David Eargle, Kirk Ouimet, and Detmar Straub. Enhancing Password Security through Interactive Fear Appeals: A Web-based Field Experiment. In *Hawaii International Conference on System Sciences*, pages 2988–2997, Maui, HI, USA, January 2013. IEEE. doi:10.1109/HICSS.2013.196.

[116] Ashlee Vance. If Your Password Is 123456, Just Make It HackMe, January 2010. https://www.nytimes.com/2010/01/21/technology/21password.html, accessed on: August 13, 2024.

[117] Rafael Veras, Christopher Collins, and Julie Thorpe. On the Semantic Patterns of Passwords and their Security Impact. In *Symposium on Network and Distributed System Security*, pages 27:1–27:16, San Diego, CA, USA, February 2014. Internet Society. https://www.ndss-symposium.org/ndss2014/programme/semantic-patterns-passwords-and-their-security-impact/.

[118] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. Targeted Online Password Guessing: An Underestimated Threat. In *ACM Conference on Computer and Communications Security*, pages 1242–1254, Vienna, Austria,

October 2016. ACM. doi:10.1145/2976749.2978339.

[119] Rick Wash, Emilee Radar, Ruthie Berman, and Zac Wellmer. Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites. In *Symposium on Usable Privacy and Security*, pages 175–188, Denver, CO, USA, July 2016. USENIX. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf.

[120] Rick Wash, Emilee Rader, and Chris Fennell. Can people self-report security accurately? agreement between self-report and behavioral measures. In *ACM Conference on Human Factors in Computing Systems*, pages 2228–2232, Denver, CO, USA, May 2017. ACM. doi:10.1145/3025453.3025911.

[121] Thomas L Webb and Paschal Sheeran. Does changing behavioral intentions engender behavior change? a meta-analysis of the experimental evidence. *Psychological Bulletin*, 132(2):249–268, 2006. doi:10.1037/0033-2909.132.2.249.

[122] Neil D Weinstein. Testing four competing theories of health-protective behavior. *Health Psychology*, 12(4):324–333, 1993. doi:10.1037/0278-6133.12.4.324.

[123] Daniel Lowe Wheeler. zxcvbn: Low-Budget Password Strength Estimation. In *USENIX Security Symposium*, pages 157–173, Austin, TX, USA, August 2016. USENIX. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_wheeler.pdf.

[124] Kim Witte and Mike Allen. A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health education & behavior*, 27(5):591–615, 2000. doi:10.1177/109019810002700.

[125] Michael Workman, William H Bommer, and Detmar Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6):2799–2816, 2008. doi:10.1016/j.chb.2008.04.005.

[126] Justin Wu and Daniel Zappala. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Symposium on Usable Privacy and Security*, pages 395–409, Baltimore, MD, USA, August 2018. USENIX. https://www.usenix.org/system/files/conference/soups2018/soups2018-wu.pdf.

[127] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *ACM Conference on Human Factors in Computing Systems*, pages 194:1–194:14, Glasgow, Scotland, UK, May 2019. ACM. doi:10.1145/3290605.3300424.

[128] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Symposium on Usable Privacy and Security*, pages 197–216, Baltimore, MD, USA, August 2018. USENIX. https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf.

[129] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *ACM Conference on Human Factors in Computing Systems*, pages 443:1–443:15, Honolulu, HI, USA, April 2020. ACM. doi:10.1145/3313831.3376570.

## A  SURVEY MATERIAL

### A.1  Screening Survey

*Informed consent. [This informed consent form was for the screening survey. We used a very similar consent form for the main and follow-up surveys, except adjusting the estimated completion time and compensation.]*

**Study Title:** Consumers' Reactions Toward Data Breaches

**Principal Investigators:** *REDACTED*

**Purpose of this Study:** We are conducting a research study to understand how consumers perceive and react to data breaches.

**Description of your involvement:**

If you agree to be part of the research study, we will ask you to complete a screening survey that asks you to provide an email address. We will query this email address in haveibeenpwned.com, a public database, to see if it has appeared in any data breaches.

Depending on the query results, we may send you an invitation to our main survey following your completion. The main survey will show more information about these breaches and ask you to answer a few questions about them.

**Compensation:**

We expect this screening survey to take **about two to three minutes**. You will be compensated **$0.80** upon completing the survey.

You are free to withdraw at any time. However, you will not be compensated if you withdraw from the study.

**Benefits and Risks:** Although you may not directly benefit from participating in this study, the study will inform how to better protect consumers against data breaches.

The risks associated with your participation are similar to those normally encountered when using the Internet. We take strong measures to protect your personal information, as we outline in the "Confidentiality" section.

**Confidentiality:** By participating in the study, you understand and agree that the *REDACTED* may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court order.

Otherwise, your confidentiality will be maintained in the following manner:

- Your data will be stored in password-protected cloud services and will only be accessible to the study team.
- We plan to publish the results of this study, but we will not include any information that would identify you.
- Throughout the study, you will not be asked to provide any direct personal identifiers in the study apart from your email address. **We do not track your email address, and we will not be able to tie your email address to any results or analysis. All records of your email address will reside in temporary storage to facilitate the lookup of data breaches, and will be deleted following the completion of this task. We will never see your actual email address.**

**Right to Ask Questions & Contact Information:** If you have questions about this research, you may contact the study team at *REDACTED*.

The *REDACTED* Institutional Review Board has determined that this study is exempt from IRB oversight.

**Voluntary Consent:** By proceeding to the next page, you are agreeing to participate in this study. You may print a copy of this consent form for your records. You may also contact the study team at any time by emailing *REDACTED* if you think of a question later.

Are you 18 years of age or older? ○ Yes    ○ No

Are you physically living in the United States? ○ Yes    ○ No

*[Participants need to answer "Yes" for both questions to proceed to the next page. If the answer is "No" to any question, show an error message "We're sorry, but to participate in this survey you must be at least 18 and currently physically located in the United States. Thank you for your interest."]*

*Breach lookup.* We are going to ask you to enter your most commonly used email address at the bottom of this page. We will use your email address to look up whether your email address has appeared in any data breaches (also called "security breaches"), using the public lookup service for data breaches haveibeenpwned.com. Based on the results, we may invite you to our main survey in which we will show you more information about these breaches.

**Privacy Notice: We do not track or store your email address as part of this study, and we will not be able tie your email address to any results or analysis.** All records of your email address will reside in temporary storage to facilitate the lookup of data breaches, and will be deleted following the completion of this task. We will never see your actual email address.

To access information about breaches, your email address will be communicated to haveibeenpwned.com, a public service that maintains a database of data breaches involving email addresses. Communication with haveibeenpwned.com will occur on secure and encrypted channels. haveibeenpwned.com does not permanently store email addresses used in queries as described in their privacy policy.

If you have any further concerns about providing your email address, you may opt-out of the survey at this time. We will remove any record of your participation. Note that if you choose to opt out, you will not be compensated.

(1) Please enter your most commonly used email address. After the task, you may search for another email address, but for now, we are primarily interested in breaches that may have involved your most commonly used email address. [free text]

*Email-related questions.* Please tell us more about this email address.

(2) Whose email address is it? ○ It is my own account / I have sole ownership of this account ○ It is my shared account / I share the account with someone else (e.g., a partner or family member)  ○ It is someone else's account / someone else has sole ownership of this account ○ I made up an email address just for this study

(3) How often do you check emails in this account? ○ Every day  ○ A few times a week  ○ A few times a month  ○ A few times a year or less frequently

(4) What do you use this email account for? Choose all that apply. ○ For personal correspondence (e.g., friends and family members)  ○ For professional correspondence (e.g., with colleagues, business partners)  ○ Sign up for sensitive accounts (e.g., banking, taxes)  ○ Sign up for medium sensitive accounts (e.g., social media, online shopping)  ○ Sign up for low-value accounts (I used it when I'm prompted to sign up but don't really care)  ○ Other [free-text]

(5) How long have you been using this email account? [number entry] ○ year(s)  ○ month(s)  ○ week(s)  ○ day(s)

(6) How many other email addresses/accounts do you regularly use? (Not counting the one you entered) [number entry]

(7) Prior to our study, have you ever checked if this email address has appeared in any data breaches using Have I Been Pwned (haveibeenpwned.com) or other services? ○ Yes  ○ No  ○ Unsure

*Demographics-related questions.* As the final part of this survey, please tell us a few things about yourself.

(8) What is your age? [number entry or "prefer not to say"]

(9) What is your gender? ○ Man  ○ Woman  ○ Non-Binary  ○ Prefer to self-describe: [free text] ○ Prefer not to say

(10) What is the highest level of education you have completed? ○ Less than high school  ○ High school or equivalent  ○ Some college, no degree  ○ Associate's degree, occupational  ○ Associate's degree, academic  ○ Bachelor's Degree  ○ Master's Degree  ○ Professional degree  ○ Doctoral degree  ○ Prefer not to say

(11) Have you studied or worked in the field of computer science or information technology? ○ Yes  ○ No  ○ Prefer not to answer

(12) Have you studied or practiced law or other legal services? ○ Yes  ○ No  ○ Prefer not to answer

(13) What was your total household income before taxes during the past 12 months? ○ Under $15,000  ○ $15,000 to $24,999  ○ $25,000 to $34,999  ○ $35,000 to $49,999  ○ $50,000 to $74,999  ○ $75,000 to $99,999  ○ $100,000 to $149,999  ○ $150,000 or above  ○ Prefer not to say

(14) Which of the following best describes you? Choose one or more. ○ White  ○ Black or African American  ○ Asian  ○ American Indian or Alaska Native  ○ Native Hawaiian or other Pacific Islander  ○ Middle Eastern or North African descent  ○ Prefer to self-describe: [free text]

(15) Are you Hispanic or Latino? ○ Yes  ○ No  ○ Prefer not to say

*Next steps (only for eligible participants).* We will send you the link to our main survey within the next week. In the main survey, we will show you more details about the data breach records associated with your provided email address.

Please click the "continue" button to proceed to the next page, where you will be automatically redirected to Prolific.

Stay tuned, and we look forward to seeing you back!

*Debrief (only for ineligible participants). [For participants who did not have any password breach but had other data breaches associated with their provided email address:]*
Thank you for completing our screening survey. We're looking for participants who have at least one password breach (i.e., a data breach that exposes users' account passwords) to take our main survey. According to haveibeenpwned.com, your email address has not appeared in any password breach.

That being said, your email address has appeared in the following data breaches, and we suggest that you take necessary precautions. Please note that you can always obtain the same results by checking your email address on haveibeenpwned.com, which, in addition, provides records with sensitive breaches upon the verification of your email account. Please keep in mind that this list only reflects breaches that are registered in the haveibeenpwned.com database, your information may have been exposed in other breaches.

*[For participants who did not have any data breach with their provided email address:]*
Thank you for completing our screening survey. We're looking for participants who have at least one password breach (i.e., a data breach that exposes users' account passwords) to take our main survey. According to haveibeenpwned.com, your email address has not appeared in any data breach.

That's great news! However, we still recommend that you monitor breach services like haveibeenpwned.com in case new breaches come to light. In case you still want to learn about what to do when you're affected by a breach, you can find several resources below.

*[For all ineligible participants:]*
Below is a list of resources to help you better protect yourself from data breaches.

- Resources about recovering from a data breach:
  - Federal Trade Commission: Identity theft recovery steps
  - Federal Trade Commission: Credit Freeze FAQs
  - Firefox Monitor: What to do after a data breach
  - Norton: What to do after 5 types of data breaches
- Resources about protecting yourself against future breaches:
  - Firefox Monitor: How to create strong passwords
  - Firefox Monitor: Steps to protect your online identity

## A.2  Main Survey

*Show breach.* In our previous survey, you provided an email address for querying the Have I Been Pwned (haveibeenpwned.com, referred to as "HIBP" onward) database for data breach records. Below is a data breach in which your provided email address has appeared. *[Show breach information.]*

*Breach-related questions.*
(16) Prior to our study, have you ever heard of [site name]? ○ Yes  ○ No  ○ Unsure
(17) Prior to our study, were you aware that you are affected by the [site name] data breach? ○ Yes  ○ No  ○ Unsure
(18) To your knowledge, do you have an account with [site name]? ○ Yes, I created an account by providing an email address and a password  ○ Yes, I created an account through a third-party

service (e.g., "sign in with Google" or "sign in with Facebook")    ○ No, I did not have an account with [site name]

(19) *[If "unsure" for Q16/Q17/Q18]* You selected unsure for [Q16/Q17/Q18]. Please explain why you selected "unsure." [free text]

(20) *[If "yes" for Q18]* To the best of your memory, how long have you been using your [site name] account? [number entry]  ○ year(s)  ○ month(s)  ○ week(s)  ○ day(s)

(21) *[If "yes" for Q18]* How often do you use your [site name] account?  ○ Every day  ○ A few times a week  ○ A few times a month  ○ A few times a year or less frequently

(22) *[If "yes" for Q18]* To the best of your memory, does your [company name] account have any of the following information about you? Please select all that apply.  ○ Date of birth  ○ Financial information (e.g., bank accounts or credit card numbers  ○ Gender  ○ IP address  ○ Name  ○ Phone number  ○ Residential address

(23) *[If "yes" for Q18]* Is there any other type of information the account may have about you? If you cannot think of any, please write "I don't know." [free text]

(24) *[If "yes" for Q18]* How important or unimportant is your [site name] account to you?  ○ Very unimportant  ○ Unimportant  ○ Somewhat unimportant  ○ Neither important nor unimportant  ○ Somewhat important  ○ Important  ○ Very important

*Measuring password change intention. [Show intervention, see Figures 1 and 2 for the specific text.]*

(25) After learning about this breach, do you intend to change the password of your [site name] account?  ○ Yes, I intend to change the password of my [site name] account  ○ No, I do not intend to change the password of my [site name] account  ○ I have already changed the password of my [company name] account after this breach occurred (on [date]) and before taking this survey

(26) Please explain why you selected this answer option. [free text]

(27) Do you use your [site name] account's password for any other online accounts?  ○ Yes  ○ No  ○ I don't know  ○ I don't have an account with [site name]

*Measuring PMT constructs. [The order of questions in this section was randomized.]*

(28) Please rate to what extent the following incidents would be a serious problem to you. [Answer options for each: not at all serious, slightly serious, somewhat serious, serious, extremely serious.]  ○ Experience financial loss  ○ Have my personal information sold to marketers  ○ Have my online accounts hacked by someone  ○ Have my identity stolen by someone  ○ Receive more spam emails  ○ Please select "extremely serious" (this is an attention check)

(29) As a result of the [site name] data breach, how likely or unlikely do you think you are to experience the following incidents? [Answer options for each: very unlikely, somewhat unlikely, neither likely nor unlikely, somewhat likely, very likely.]  ○ Experience financial loss  ○ Have my personal information sold to marketers  ○ Have my online accounts hacked by someone  ○ Have my identity stolen by someone  ○ Receive more spam emails  ○ Please select "very unlikely" (this is an attention check)

(30) Please rate your level of disagreement or agreement with the following statement: "Changing the password of my [site name] account will protect me from negative incidents as a result of the [site name] breach."  ○ Strongly disagree  ○ Somewhat disagree  ○ Neither agree nor disagree  ○ Somewhat agree  ○ Strongly agree

(31) How easy or difficult do you think it would be for you to change the password of your [site name] account?  ○ Very difficult  ○ Somewhat difficult  ○ Neither easy nor difficult  ○ Somewhat easy  ○ Very easy

(32) If I were to change the password of my [site name] account, I would... [Answer options for each: not true at all, slightly true, somewhat true, true, extremely true.]  ○ Spend a lot of time

changing the password    ◦ Changing the password requires me to learn new skills    ◦ Feel more anxious about the [site name] data breach    ◦ Forget the new password and be locked out of the account

*SA-6 & prior negative experience.* You're almost done! Just a few questions about yourself.

(33) Please indicate your agreement with the following statements. [Answer options for each: strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, strongly agree.] ◦ Generally, I diligently follow a routine about security practices.    ◦ I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.    ◦ I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.    ◦ I am extremely motivated to take all the steps needed to keep my online data and accounts safe.    ◦ I often am interested in articles about security threats.    ◦ I seek out opportunities to learn about security measures that are relevant to me.

(34) Has anyone ever gained unauthorized access to one of your online accounts? E.g., someone secretly changed your password without you noticing it. ◦ Yes    ◦ No    ◦ Unsure

(35) Have you ever learned that your information was exposed in a data breach before taking our survey? ◦ Yes    ◦ No    ◦ Unsure

(36) Have you ever been a victim of identity theft? E.g., someone secretly applied for a new credit card under your name. ◦ Yes    ◦ No    ◦ Unsure

(37) *[If "unsure" for Q34/Q35/Q36]* You selected unsure for [Q34/Q35/Q36]. Please explain why you selected "unsure." [free text]

*Final remarks.* Thank you for completing this survey! Please note that the information about this data breach we showed to you is real. Your email address and potentially other personal information has appeared in this breach and could be used by criminals to steal your identity or access your online accounts.

You can check a full list of data breaches associated with your email address on haveibeenpwned.com, which, in addition, provides records with sensitive breaches upon the verification of your email account. Please keep in mind that this list only reflects breaches that are registered in the haveibeenpwned.com database, your information may have been exposed in other breaches.

Please click the "continue" button to proceed to the next page, where you will be automatically redirected to Prolific.

## A.3   Follow-up Survey

*Reminder of breach.* In our previous survey, you provided an email address for querying the Have I Been Pwned (haveibeenpwned.com, referred to as "HIBP" onward) database for data breach records.

Below is a data breach in which your provided email address has appeared.

*[Show breach information.]*

(38) Since taking our previous survey on [date], what did you do, if anything, after learning that your information was exposed in the [site name] data breach? Please explain why. [free text]

*Attention check.*

(39) This is an attention check. What is the name of the company that suffered a data breach and exposed your information, as we show you in the previous page? ◦ correct answer    ◦ AKP emails    ◦ KnownCircle    ◦ Staminus

*Measuring password change behavior.*

(40) You took our previous survey on [date]. The survey showed that your information was exposed in the [site name] data breach. Since then, have you changed the password for your [site name] account? ◦ Yes    ◦ No

(41) Please explain why you changed or did not change your [site name] account's password after taking our previous survey on [date]. [free text]

(42) What did you do about passwords for other accounts? ○ I changed the password for every online account I have    ○ I changed the password for other accounts that use the same or similar passwords    ○ I changed the password for really important accounts (e.g., bank accounts)    ○ I kept using the same password for other accounts

(43) *[If "Yes" for Q40]* To your best estimate, how soon after taking our previous survey on [date] did you change the password for your [site name] account? [number entry] days

(44) *[If "Yes" for Q40]* What did you use for the new password for your [site name] account? ○ A password that I already use for other accounts    ○ Something related to the old password but a few characters different, created by myself    ○ Something completely unrelated to the old password, created by myself    ○ A unique or random password, such as one generated by a password manager    ○ Other: [free text]

(45) *[If "Yes" for Q40]* What techniques did you use to remember the new password for your [site name] account? Please select all that apply.  ○ I remembered my new password without writing it down or storing it digitally    ○ I reset my password every time I log in rather than remembering my new password    ○ I wrote my new password down on paper or other physical media    ○ I stored my new password in a digital file or files    ○ I saved my new password in the browser (e.g., passwords saved in Chrome)    ○ I used a system-provided password manager (e.g., Apple's Keychain)    ○ I used a third-party password manager (e.g., 1Password or LastPass)    ○ Other: [free text]

*Screenshot upload. [Only display this page if "yes" for Q40.]*

Optional: Please upload a screenshot of the password reset confirmation email you received from [site name] after changing the password. Make sure the image you are uploading is in PNG format. We would greatly appreciate it if you do this, as it will help us validate your responses.

If you upload a valid screenshot upon our verification, you will receive a $1.00 bonus payment in addition to the $1.20 base payment.

Steps to take:

- Sign in to your email account; make sure this account has the email address you checked for breaches in our earlier survey.
- Do a keyword search of "[site name]" in your inbox and/or spam folder.
- On a Windows PC, open the "Snipping Tool" program; on a Mac computer, press Shift + Command + 4 on your keyboard to take a screenshot.
- Select the area you want to take a screenshot of. Make sure your screenshot includes the email's subject line, sender, and date (see the example below).
- **IMPORTANT: Do NOT upload a screenshot that includes your personal information, such as your actual email address, username, and new password.**

(46) Which of the following options applies to you? ○ I have my screenshot and I am ready to upload it on the next page.    ○ I cannot find the password reset confirmation email (please explain why): [free text]    ○ I choose not to upload the screenshot (please explain why): [free text]

*Final remarks.* Thank you for your participation! As we noted in our previous surveys, the information about the data breach we showed to you is real. Your email address and potentially other personal information has appeared in this breach and could be used by criminals to steal your identity or access your online accounts.

Below is the full list of breaches associated with the email address you provided. Please note that you can always obtain the same results by checking your email address on haveibeenpwned.com,

which, in addition, provides records with sensitive breaches upon the verification of your email account. Please keep in mind that this list only reflects breaches that are registered in the haveibeenpwned.com database, your information may have been exposed in other breaches.

[Show all breaches.]

- Resources about recovering from a data breach:
  - Federal Trade Commission: Identity theft recovery steps
  - Federal Trade Commission: Credit Freeze FAQs
  - Firefox Monitor: What to do after a data breach
  - Norton: What to do after 5 types of data breaches
- Resources about protecting yourself against future breaches:
  - Firefox Monitor: How to create strong passwords
  - Firefox Monitor: Steps to protect your online identity

We greatly appreciate the insights you contributed, which would help us develop better technologies and interfaces that notify people of data breaches.

Would you like to be contacted by us to participate in our future research? ∘ Yes, I am interested. ∘ No, I am not interested.

Please click the "continue" button to proceed to the next page, where you will be automatically redirected to Prolific.

## B COGNITIVE WALKTHROUGH PROTOCOL

*Introduction.* Today we will be testing a series of three surveys for an experiment. To ensure you have a fresh experience, I will not reveal the experiment's purpose, but I am happy to talk about it toward the end.

The first survey is a screening survey. You will be asked to provide an email address for querying a database and see if this email address has appeared in any data breaches.

The second survey is the main survey. You will see more information about a breach associated with the email address you provided, and answer some questions about it.

The third survey is a follow-up survey. For real-world participants, they will receive a link to this survey two weeks after the second survey. Since we are doing pilot testing today, I will ask you to review the follow-up survey as well.

The link to all surveys is [URL]. If possible, could you please share your screen with me as you complete the surveys? We'll be using a think-aloud protocol, which means you will read out the survey questions on your screen line by line, tell me your answer and why you select it. Please also feel free to comment on your thoughts and reactions to the survey questions, especially if there's anything that's unclear or doesn't make sense to you.

For most of the time, I will be quietly sitting in the background and observe your interactions. I may chime in if there is a critical question I want to ask on the spot. I also have a list of questions I would like to get your feedback on toward the end after you complete all three surveys.

I will be taking notes as I observe your interactions. However, to make sure I capture everything, would you mind me recording our meeting today as well?

*Questions to ask.*
- Does the text under "What are the risks" describe the threats clearly? Does the text under "How to change your password" provide useful information? Do you feel motivated to change an exposed password after reading the text?
- Right now there's a 2-second delay after "What to do" and a 10-second delay after the threat/coping module. The delay seeks to nudge participants to pay close attention to the text while waiting. Is the delay too long, too short, or just the right amount for you?

- For the follow-up survey, how's your experience of completing the screenshot upload question? Are the instructions clear? Is this question in line with ethical data collection? Are they written in a way that minimizes accidental information leaks from taking screenshots of emails?
- Any unclear or confusing wording for any survey questions?

## C   BREACHES IN OUR SAMPLE
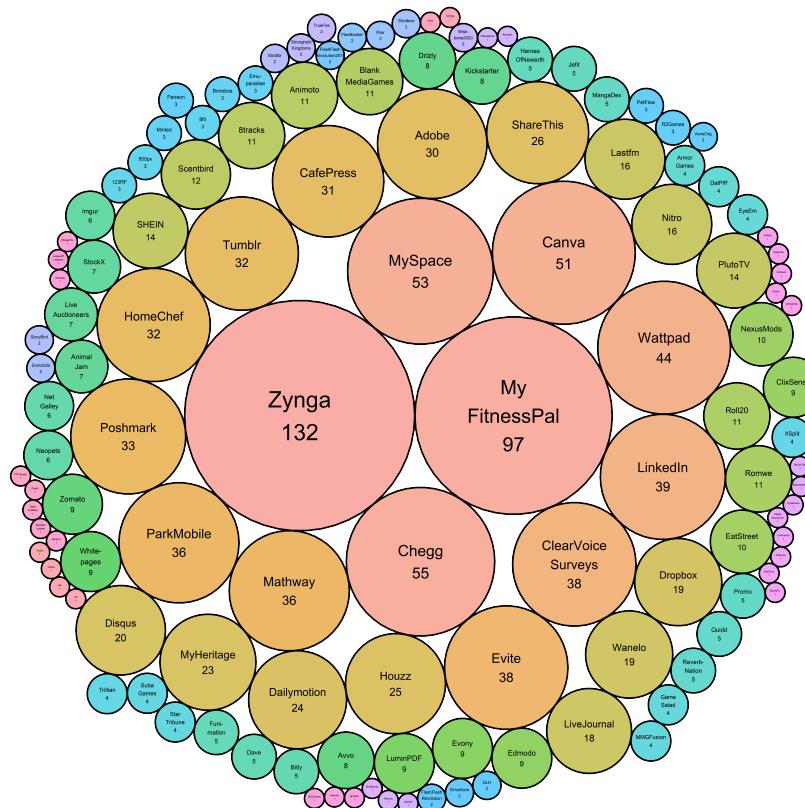


Fig. 5.  Company name and frequency of the breaches featured in our study (bubble size proportionate to each breach's frequency).
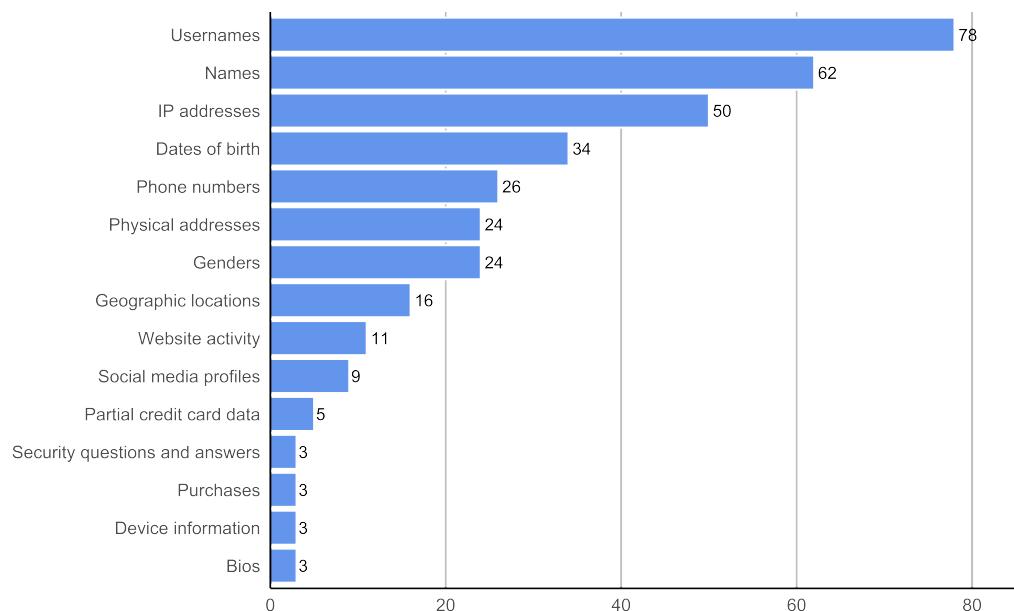
Fig. 6. How often each data type got leaked among the 127 breaches in our sample, excluding email addresses and passwords (appearing in all breaches). Eliminated 26 other types occurring twice or fewer.

## D MANIPULATION CHECK RESULTS

| Variable | Condition | Mean | Median | SD |
|---|---|---|---|---|
| Threat severity | Control | 4.28 | 5.00 | 0.90 |
| | Threat only | 4.37 | 5.00 | 0.79 |
| | Coping only | 4.31 | 4.50 | 0.88 |
| | Combined | 4.32 | 4.00 | 0.83 |
| Threat vulnerability | Control | 2.73 | 3.00 | 0.06 |
| | Threat only | 2.99 | 3.00 | 0.06 |
| | Coping only | 2.89 | 3.00 | 0.06 |
| | Combined | 3.01 | 3.00 | 0.06 |
| Self-efficacy | Control | 3.99 | 4.00 | 1.14 |
| | Threat only | 3.96 | 4.00 | 1.15 |
| | Coping only | 4.04 | 4.00 | 1.13 |
| | Combined | 4.00 | 4.00 | 1.07 |
| Response efficacy | Control | 3.20 | 3.00 | 1.13 |
| | Threat only | 3.44 | 4.00 | 1.15 |
| | Coping only | 3.28 | 4.00 | 1.17 |
| | Combined | 3.55 | 4.00 | 1.13 |
| Response costs | Control | 1.51 | 1.00 | 0.74 |
| | Threat only | 1.52 | 1.00 | 0.79 |
| | Coping only | 1.51 | 1.00 | 0.79 |
| | Combined | 1.60 | 1.50 | 0.80 |

Table 8. Mean, median, and standard deviation of participants' rating of the PMT constructs, divided by conditions. We adapted scales from prior work [9, 99] in measuring these variables: threat severity (Q28), threat vulnerability (Q29), response costs (Q32) were measured using 5-point Likert scales, taking the median. Response efficacy (Q30) and self-efficacy (Q31) were measured using a single 5-point Likert-type item.

# E QUALITATIVE CODEBOOK

We provide our codebook for each coded question as well as the respective count for each code.

## E.1 Password Change Intention (Main Survey, Q26)

● **Yes (868)**: *to be safe (223), bad things (212), take other actions (181), inactive use (103), triggered by breach (98), action good idea (65), reuse passwords (47), depend on account access (40), just changed Password (40), forget password (24), yes sensitive info (23), other existing measures (19), action easy (18), instructed by survey (18), unspecific (18), action important (17), tried and failed (17), no sensitive info (16), unsure if already changed (16), no account (15), unaware account existence (15), prior negative experience (14), unsure account existence (14), distrust company (13), resigned (11), use unique passwords (9), don't know site (8), important account (8), unsure about info in account (8), forget account existence (7), unimportant password (7), already changed password (6), account future use (6), old breach (5), limited impact (4), account created via social login (3), unimportant email (1)* ● **No (518)** *inactive use (189), no account (152), sensitive info no (80), forget password (45), take other actions (45), unimportant password (43), unimportant account (42), limited impact (29), tried and failed (28), resigned (23), use unique passwords (23), already changed password (21), don't know site (19), too much effort (18), unsure account existence (18), old breach (16), other existing measures (13), don't know how (8), reuse passwords (8), account created via social login (8), unaware account existence (8), unspecific (8), distrust company (7), distrust intervention (5), forget account existence (5), unimportant email (5), prior negative experience (3)*

## E.2 Actions Taken (Follow-up Survey, Q38)

● **Action (632)**: *change this password (214), change other passwords (171), delete this account (89), try accessing account but fail (89), check breach records (59), check reused passwords (48), check/delete info in account (35), check out the breached site (32), review other accounts (27), check info leaked in this breach (20), enable two-factor authentication (19), other miscellaneous action (11), research on cybersecurity (11), unsubscribed (10), inform others (9), start to use password managers (9), check credit reports (8), use credit monitoring services (8), check financial statements (7), use antivirus (6), use stronger passwords (5), be careful with emails (4), create a new email (4), delete other accounts (4), stay vigilant (4)* ● **Nothing (543)**

## E.3 Password Change Behavior (Follow-up Survey, Q41)

● **Yes (855)**: *to be safe (96), bad things (72), trigger by breach (42), take other actions (41), inactive use (20), to access account (18), instructed by survey (16), reuse passwords (15), action easy (12), action good idea (11), change passwords regularly (10), no sensitive info (10), yes sensitive info (9), distrust company (8), already changed password (7), refer to intervention text (7), use password managers (7), unspecific (6), use unique passwords (5), resigned (3), action important (2), account future use (2), prior negative experience (2), don't know site (1), limited impact (1)* ● **No (320)** *inactive use (282), no account (169), no sensitive info (86), tried and failed (86), forget to do (78), take other actions (75), unimportant account (67), forget password (59), unimportant password (39), busy (38), don't know site (24), limited impact (24), too much effort (24), use unique passwords (20), already changed password (19), action unnecessary (17), unspecific (15), distrust company (14), resigned (12), not a priority (9), old breach (9), account created via social login (8), unsure account existence (3), use password managers (3), change passwords regularly (2)*