Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches*

PETER MAYER, University of Southern Denmark, Denmark and Karlsruhe Institute of Technology, Germany
YIXIN ZOU, Max Planck Institute for Security and Privacy, Germany
BYRON M. LOWENS, University of Michigan, USA
HUNTER A. DYER, The George Washington University, USA
KHUE LE, University of Michigan, USA
FLORIAN SCHAUB, University of Michigan, USA
ADAM J. AVIV, The George Washington University, USA

Data breaches are prevalent. We provide novel insights into individuals' awareness, perception, and responses to breaches that affect them through two online surveys: a main survey (n=413) in which we presented participants with up to three breaches that affected them, and a follow-up survey (n=108) in which we investigated whether the main study participants followed through with their intentions to act. Overall, 73% of participants were affected by at least one breach, but participants were unaware of 74% of breaches affecting them. While some reported intention to take action, most participants believed the breach would not impact them. We also found a sizeable intention-behavior gap. Participants did not follow through with their intention when they were apathetic about breaches, considered potential costs, forgot, or felt resigned about taking action. Our findings suggest that breached organizations should be held accountable for more proactively informing and protecting affected consumers.

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, privacy, security, perception, awareness, emotion, behavior.

1 Introduction

According to a 2019 report [30], the average user has accounts with 191 online services that require them to enter passwords or other credentials. These online accounts are at risk when data breaches — the disclosure of sensitive personal information to unauthorized parties — take place. Breach notification services such as Have I Been Pwned (HIBP) give insights into the extent and frequency of such data breaches. At the time we conducted this research, the Have I Been Pwned (HIBP) breach database listed over 480 breached online services

*This is an extended version of the original research paper: Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. 2021. ""Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them." 30th USENIX Security Symposium (USENIX Security 21).

Authors' addresses: Peter Mayer, peter.mayer@kit.edu, University of Southern Denmark, Denmark and Karlsruhe Institute of Technology, Germany; Yixin Zou, yixin.zou@mpi-sp.org, Max Planck Institute for Security and Privacy, Germany; Byron M. Lowens, bmlowens@umich.edu, University of Michigan, USA; Hunter A. Dyer, hdyer@gwmail.gwu.edu, The George Washington University, USA; Khue Le, khuele@umich.edu, University of Michigan, USA; Florian Schaub, fschaub@umich.edu, University of Michigan, USA; Adam J. Aviv, aaviv@gwu.edu, The George Washington University, USA.

1073-0516/2023/4-ART $15.00
https://doi.org/10.1145/3589958

	Total	Num. (%) W/ Breaches	Num. (%) W/o Breaches	Avg. (Med./Std.) Breaches
Men	**199**	139 (70%)	60 (30%)	4.49 (2/5.97)
Women	**212**	162 (76%)	50 (24%)	6.11 (4/6.28)
Non-Binary	**2**	1 (50%)	1 (50%)	11.00 (11/11.00)
18-24	**77**	56 (73%)	21 (27%)	3.90 (2/5.15)
25-29	**51**	35 (69%)	16 (31%)	4.25 (2/4.90)
30-34	**42**	33 (79%)	9 (21%)	6.55 (3/8.72)
35-39	**49**	29 (59%)	20 (41%)	4.63 (1/7.05)
40-44	**45**	26 (58%)	19 (42%)	4.36 (2/5.04)
45-49	**32**	29 (91%)	3 (9%)	6.59 (4/6.05)
50-54	**39**	30 (77%)	9 (23%)	6.72 (6/6.16)
54-59	**34**	30 (88%)	4 (12%)	6.12 (5/4.82)
60-64	**27**	19 (70%)	8 (30%)	6.52 (3/6.85)
65+	**17**	15 (88%)	2 (12%)	8.24 (8/6.06)
Some High School	**1**	0 (0%)	1 (100%)	0.00 (0/0.00)
High School or Equiv.	**46**	35 (76%)	11 (24%)	4.59 (3/4.61)
Some College	**88**	70 (80%)	18 (20%)	5.67 (3/6.63)
Associate (voc./occ.)	**14**	14 (100%)	0 (0%)	8.07 (6/6.51)
Associate (aca.)	**20**	19 (95%)	1 (5%)	6.10 (4/5.99)
Bachalor	**140**	108 (77%)	32 (23%)	6.04 (4/6.56)
Masters	**83**	46 (55%)	37 (45%)	4.10 (2/5.68)
Professional	**5**	4 (80%)	1 (20%)	11.60 (13/7.71)
Doctorate	**16**	6 (38%)	10 (62%)	1.44 (0/2.26)
IT Background	**122**	67 (55%)	55 (45%)	3.82 (1/6.30)
No IT Background	**278**	224 (81%)	54 (19%)	5.91 (4/6.06)
Prefer not to say	**13**	11 (85%)	2 (15%)	8.00 (9/6.41)
Law Background	**25**	14 (56%)	11 (44%)	5.80 (2/9.63)
No Law Background	**374**	278 (74%)	96 (26%)	5.29 (3/5.93)
Prefer not to say	**14**	10 (71%)	4 (29%)	6.36 (5/6.25)
No Data	**170**	115 (68%)	55 (32%)	4.45 (2/6.21)
<$15K	**16**	15 (94%)	1 (6%)	7.81 (4/8.59)
$15K-$25K	**22**	20 (91%)	2 (9%)	6.77 (4/5.79)
$25K-$35K	**28**	26 (93%)	2 (7%)	5.89 (3/5.37)
$35K-$50K	**26**	19 (73%)	7 (27%)	4.58 (2/5.35)
$50K-$75K	**45**	40 (89%)	5 (11%)	8.04 (7/6.50)
$75K-$100K	**38**	28 (74%)	10 (26%)	6.95 (4/6.61)
$100K-$150K	**37**	22 (59%)	15 (41%)	4.05 (2/4.63)
>$150K	**24**	13 (54%)	11 (46%)	3.92 (2/5.34)
Total	**413**	**302 (73%)**	**111 (27%)**	**5.36 (3/6.23)**

Table 1. Participant demographics and breach status for the main survey (n=413).

and over 10 million compromised accounts [49]. Data breaches pose risks to affected consumers as their leaked information could be misused for cybercrimes such as identity theft. The Identity Theft Resource Center recorded 1,862 data compromises that occurred in the United States in 2021 with 293 million individual victims [51]. The sheer number of breaches also makes it challenging to track the total number of records involved and notify affected consumers [57, 118, 121]. Facing a plethora of data breaches [51, 94], consumers rarely take recommended protective measures in response [1, 53, 142].

Prior work has primarily studied consumers' general reactions to data breaches [1, 53, 59] or has focused on individual breaches in isolation such as the Equifax [142] and Target breaches [44, 65]. In contrast to this, we conducted an online study in which we used the HIBP database to present participants with, and have them reflect on, specific data breaches that had exposed their email addresses and other personal information. Our study consisted of two online surveys, a main survey (n=413), which we reported on in our prior work [77] and a

Table 2. Logistic regression for breach status of an email address (leaked vs. not leaked).

	Est.	OR	95% CI	p-value
(Intercept)	−1.95	0.14	[0.04, 0.49]	.002
Freq. Checked daily (vs. weekly)	0.83	2.30	[1.07, 4.99]	.03
Prof. Corr. yes (vs. no)	−0.02	0.98	[0.51, 1.87]	.94
Pers. Corr. yes (vs. no)	0.76	2.13	[1.13, 4.03]	.02
Acct. Creat. yes (vs. no)	0.31	1.36	[0.60, 3.07]	.46
Email age years	0.30	1.35	[1.26, 1.46]	< .001
Age: 35-54 (vs. 18-34)	−0.51	0.60	[0.29, 1.23]	.16
Age: 55+ (vs. 18-34)	−0.60	0.55	[0.27, 1.10]	.09
Gender: men (vs. women)	−0.24	0.79	[0.43, 1.45]	0.45
Edu.: =Bach. (vs. <Bach.)	0.25	1.28	[0.65, 2.53]	0.48
Edu.: >Bach. (vs. <Bach.)	−0.62	0.54	[0.25, 1.16]	.11
Occu.: IT/law yes (vs. no)	−0.51	0.60	[0.31, 1.17]	.14

follow-up survey (n=108), the results of which are first published in this article. In the main survey, we used the HIBP database to gather 792 detailed breach-specific responses (up to three per participant), covering 189 unique breaches and 66 different exposed data types. Our findings contribute quantitative and qualitative insights into individuals' awareness, perception, and responses to specific data breaches that affected them. In the follow-up survey, we invited participants of the main survey back after about six months and received 108 responses. We examined for which actions participants were likely to follow through with their intention to act, as stated in the main survey, and factors influencing the execution of intended actions. Both surveys were driven by research questions as outlined below. Our findings from the main survey answer the following five research questions:

RQ1 [Breach Status] *What factors influence the likelihood that an email address is involved in a data breach?*

Overall, 73% of our participants experienced at least one breach and 5.36 breaches on average. An email address's likelihood of being exposed in a breach significantly correlated with the email account's age and utilization.

RQ2 [Perception] *What do participants perceive as the causes of being involved in data breaches and related impacts, and to what extent do their perceptions align with reality?*
Only 14% of our participants accurately attributed the cause of being affected by a breach to external factors such as breached sites and hackers. Others blamed their email or security behaviors for making themselves victims or viewed breaches as inevitable. Most participants expected little impact from shown breaches despite realizing certain risks.

RQ3 [Awareness] *What factors influence participants' awareness of data breaches that affected them?*
Participants were unaware of most data breaches presented (74%). Those who knew they were affected by a specific breach had primarily learned about it from the breached site or third-party services. Participants were more likely to be aware of older rather than recent breaches.

RQ4 [Emotional Response] *What are participants' emotional responses to data breaches that affected them?*
Most participants rated their concern regarding breaches as low (56% slightly/somewhat concerned, 19% no concern). Certain breached data types such as passwords and physical addresses raised more concern than others. Participants expressed feeling upset, angry, annoyed, frustrated, surprised (or not), violated, and fatigued.

RQ5 [Behavioral Intention] *What factors influence participants' intention to take action in response to data breaches that affected them?*
Participants reported having already or being very likely to change their passwords and review credit reports/financial statements in response to over 50% of shown breaches. Participants were more likely to take action with increased concern and prior awareness, suggesting that better communication about breaches could increase individuals' tendency to take protective actions.

Additionally, our findings from the follow-up survey answer the following two research questions:

RQ6 [Actual Behavior] *To what extent do participants follow through on their intentions to take action six months after the main survey?*
Our findings show that the presence of an intention-behavior gap depends on the specific action. The most often performed actions were reviewing credit reports and/or financial statements as well as changing passwords. The least performed actions were taking legal action against the affected web service and filing a complaint with a consumer protection agency.

RQ7 [Motivators & Impediments] *What factors influence participants' execution of intended actions in response to data breaches that affected them?*
Participants' open-ended responses indicate that concern, prior incidents, and a proactive attitude toward security risks were common motivators for taking action. Apathy, perceived costs being more than potential benefits, forgetting about the incident, and a general resignation towards data breaches were common hindrances to taking action.

Our findings demonstrate the need for more proactive communications of data breaches and stronger protections for affected individuals. Rather than burdening consumers to take action, breached businesses should be held responsible for increasing consumers' awareness and providing appropriate mitigations (e.g., unique email alias generators and password managers) that can help affected individuals become more resilient against future

breaches. Our findings from the follow-up survey surface a sizeable intention-behavior gap and provide design implications for interventions that bridge such a gap. Furthermore, participants' motivators and impediments for following or not following through with their intentions suggest the need for rethinking how inaction should be viewed. We need interventions that address misconceptions and help consumers take action when they are motivated to do so. Meanwhile, we need more research to show when inaction could be rational and how to personalize advice to consumers in order to minimize their burden and help them identify actions that are most applicable to their specific situations.

2 Background and Related Work

Data breaches. Schlackl et al. [110] identified eight categories of consequences of data breaches from the literature; the consequences apply to not only the organization that suffered the breach, but also customers, competitors, supply chain partners, and other actors. Breached organizations can bear substantial costs to repair the aftermath, including forensics, patching system vulnerabilities, operational interruptions, compensations to affected individuals, and resolving potential lawsuits [5, 39, 48, 104, 106]. There are also invisible and hard-to-measure costs in rebuilding the breached organization's reputation [63, 136] and affected individuals' trust [1, 16, 18, 79]. For affected individuals, exposed data puts them at risk of account compromise [30, 97, 112, 125], phishing [90], and identity theft [3, 103, 108, 117]. Though it may take years before leaked data is misused, the harm can be profound when it happens. For instance, victims of identity theft may have ruined credit reports or have to file for bankruptcy due to abuse of credit [7]. Identity theft is also traumatizing: in a 2021 survey by the Identity Theft Resource Center (ITRC) [50], 8% of respondents reported having suicidal thoughts that they did not have before. Thus, some researchers have argued that data breaches cause compensable harm due to the substantial risk of future financial injury and the emotional distress imposed on victims [25, 117].

Breached organizations are often legally required to notify affected victims [34, 92] and offer compensations such as discounts [19] or free credit/identity monitoring [111]. Services like HIBP [49] and Firefox Monitor [83] examine third-party breach reports and notify signed-up users. Some companies automatically reset passwords for users whose credentials appeared in password dumps [43, 137]. Additional measures for victims include two-factor authentication (2FA) that increases the difficulty of misusing leaked credentials and warnings that flag social engineering and phishing attacks [71, 91]. Nevertheless, no solution is perfect: attackers can bypass 2FA without obtaining the secondary token [31, 54], and phishing warnings have low adherence rates [4, 6, 33].

Security mental models and behaviors. How individuals perceive the causes and impacts of data breaches relates to mental models of security and privacy. Mental models — an individual's internalized representation of how a system works [86] — have been studied for computer security [60, 131], security warnings [12], smart home security [66, 140], and the Internet [58]. Respective studies consistently find that unawareness and misconceptions of security risks create hurdles to adopting effective mitigation strategies. Even when individuals correctly assess risks, they may still not react accordingly due to bounded rationality and cognitive biases [2] or not having experienced negative consequences [143].

In our main survey, we investigate two aspects that may impact how individuals respond to data breaches: *awareness*, i.e., whether and how individuals learn about a breach, and *perception* regarding a breach's potential causes and impacts. For awareness, prior research has documented various channels individuals leverage to learn about security advice, including media, peers, family, workplace, and service providers [24, 96, 98]. For data breaches specifically, respondents of RAND's 2016 survey [1] reported first learning of a breach from the breached organization's notification (56%), media reports (28%), or third parties (16%). Additionally, prior research has shown that consumers understand the potential impacts of data breaches, such as identity theft and personal information leakage [53, 59, 142]. Our work complements these findings by prompting participants to reflect on

both causes and impacts of specific breaches that affected them, providing insights into how these perceptions link to their emotions and behaviors.

Consumer reactions to data breaches. Data breach victims are advised to take a range of actions depending on the information exposed [123, 124, 130], such as changing passwords if account credentials are exposed and requesting new credit cards if financial information is exposed. In the US, victims are further urged to place a credit freeze, check credit reports, and file taxes early if their Social Security number (SSN) is exposed [73, 122, 123].

Nevertheless, studies on breaches in general [1, 53, 59] and on specific breaches [44, 65, 126, 142] show that consumers rarely take recommended protective measures in response [53, 142, 143]. Consumers generally report increased concern about identity theft [8, 53] and diminished trust in the breached organization as well as their service and information quality [16, 84, 110]. Nonetheless, such risk perception and attitudinal change often do not result in action. Consumers tend to accept compensations provided by the breached organization [1, 81] but do not go further; they continue using existing credit cards [81] and the same password for different accounts [40], thereby fueling credential stuffing attacks that cause account compromises [51].

Several studies have examined the determinants of consumers' behavioral reactions to data breaches: knowledge of available measures [142], perception of clear evidence indicating being affected [80], cognitive biases [142], peer influence [21, 65], and media coverage [24]. Tech-savvy and non-tech-savvy individuals also differ in their needs for guidance related to mitigating actions [8]. Furthermore, breach notifications to victims are often ambiguous in communicating the risks of a breach and priority among recommended actions [11, 129, 141]. These issues, coupled with the overwhelming amount of security advice for end-users [99, 101], pose challenges for affected individuals to act on provided advice.

Methodologically, prior work primarily asked participants to recall past experiences with generic breaches [1, 53] or describe intended reactions in hypothetical scenarios [46, 59]. By contrast, we apply a novel approach to examine participants' responses to specific breaches that exposed their information. Our sample covers a multitude of breaches varying in size and types of exposed information rather than one breach as a case study [44, 81, 126, 142]. Our approach increases ecological validity and mitigates recall bias as participants are confronted with breaches that affected them. Similar reflection studies have yielded insights into users' attitudes and behaviors in other contexts, such as password creation behaviors [89, 132] and reactions to online tracking [135] or advertising inference [95].

The intention-behavior gap. Much existing security and privacy research has used behavioral intention as a proxy for actual behavior due to difficulties in observing the latter [72]. However, research in other domains such as personal health has revealed an intention-behavior gap. 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 [134]. Sheeran and Webb summarized three key challenges that people may encounter as they strive to enact their intentions [113]: (1) fail to get started (e.g., forget to act or miss opportunities to act); (2) fail to keep goal pursuit on track (e.g., get derailed by competing goals); and (3) fail to bring goal pursuit to a successful close (e.g., fall short of the desired outcome). Correspondingly, there are self-regulatory mechanisms that target these challenges to help people realize their intentions, such as forming implementation intentions [41] and monitoring goal progress [45].

Among the limited number of studies that examined the intention-behavior gap in security contexts, Crossler et al. found that the costs of implementation (e.g., in terms of time and inconvenience) could be a strong deterrent to full compliance for employees to follow Bring Your Own Device policies [20]. Similarly, Jenkins et al. found that high levels of required effort negatively moderated users' intentions to follow security policies [56]. In the privacy literature, Norberg et al. [85] were the first to demonstrate the intention-behavior gap by showing that people are more likely to share personal information than they intend to during marketing exchanges; the authors coined the term "privacy paradox" to describe this phenomenon. The privacy paradox remains a

topic of debate, since some studies found a positive correlation between intention and behavior with large effect sizes [29, 61], and others found a reversed intention-behavior gap where participants disclosed less information in the behavior condition than in the intention condition [120]. Research on the underlying mechanisms of the concern-behavior gap [10] (which might also explain the intention-behavior gap) argues that the gap could occur after an explicit risk-benefit calculation (which could be biased or unbiased), or individuals may engage in little or no risk assessment due to a lack of knowledge [2] and learned helplessness [115]. Our work contributes to the literature by studying the existence of the intention-behavior gap (or not) in people's reactions to data breaches, a context that has not been studied before. Notably, we relied on participants' self-reported data rather than observing their behaviors. While this measurement of actual behavior was not perfect, we were able to identify the motivations and hurdles behind the translation from intention to behavior by probing participants to reflect on their experience between the two surveys.

3 Methods

In this section, we describe the survey protocol, recruitment, and data analysis procedure for the main and follow-up surveys respectively. We also report the sample of each survey and reflect on our research's limitations. Both surveys were approved by the Institutional Review Boards (IRB) at the University of Michigan and the George Washington University.

3.1 Method: Main Survey

Our main survey addresses the following five research questions. To identify what factors influence an email address's likelihood of being involved in a breach (RQ1), we collected details about participants' email usage and demographics. To identify perceptions regarding the causes of being involved in a breach and related consequences (RQ2), we asked participants to speculate why their email address may have or have not been involved in any data breaches, and any associated impacts they expect or have experienced. For each specific breach, we asked participants if they were previously aware of it and, if so, how (RQ3). To assess emotional responses, we asked participants to describe how they feel about the breach and rate their concern (RQ4). We further asked participants to self-report what they did in response to the breach and rate the likelihood of taking (or having taken) ten provided actions (RQ5). We ran regression models to examine the relationship between email usage, breached data types, awareness, concern, and behavioral reactions.

3.1.1 Survey Instrument. To understand participants' responses to real-world breaches at scale, we pulled information about data breaches from Have I Been Pwned (HIBP).[1] We built a survey platform that queried the HIBP web service API using email addresses provided by study participants. To protect participants' confidentiality, we only maintained email addresses in ephemeral memory to query HIBP. At no point did we store participants' email addresses. We then used the query results, i.e., the breaches in which a participant's email address was exposed, to drive the remainder of the survey. Appendix A includes the full survey instrument, divided into three parts. The survey instrument was piloted with colleagues and students from our research labs, who were not involved in the project.

Part 1: Email address-related questions. After consenting, we asked participants for their most commonly used email addresses. We clearly noted that the email address will only be used to query HIBP and that we will never see it (Appendix A.2). Once a participant entered an email address, we asked a few questions about it. Participants who indicated that the email address belonged to someone else or was fabricated were given the option to enter a different email address or leave the study. Next, we asked participants about their email habits as a potential influencing factor of the email's involvement in breaches (RQ1). This included frequency of checking the email,

[1] https://haveibeenpwned.com

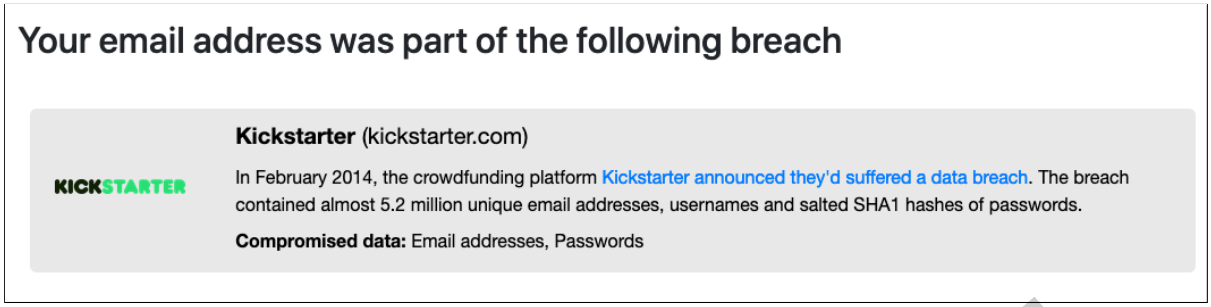


Fig. 1. Sample breach information shown to participants.

the primary use of the account (professional/personal correspondence or account creation), how long it has been used, and the number of other email accounts the participant used. We then used the provided email address to query HIBP.

Part 2: Breach-related questions. We next informed participants whether their email address was exposed in any data breaches without stating the specific number or giving more details. To answer RQ2, we asked participants to speculate why their email address was or was not part of data breaches. Participants whose email address was not part of any breach were given the opportunity to enter a different email address until a provided email address had associated breaches. If they did not provide another email, they continued with Part 3.

We randomly selected up to three breaches, displayed one by one, to ask breach-related questions while limiting potential fatigue. We displayed a breach's description, logo, name, and types of compromised data as provided by HIBP (Figure 1). We explicitly stated that these were actual breaches, and no participants doubted the validity of shown breaches in their qualitative responses. For each breach, we asked about participants' awareness (RQ3), emotional response (RQ4), and actions taken or intended to take (RQ5). For emotional response, participants provided open-ended responses, then rated their concern level on a 5-point Likert item regarding the breach in general and for each type of exposed data. For behavioral response, participants described their reactions in free-text responses before rating their intention to take (or whether they had taken) ten provided actions sourced from prior work [123, 124, 130]. The respective breach information was visible at the top of the page when participants answered all these questions.

Part 3: Demographics, attention check, and debrief. We collected participants' demographics including age, gender, education, whether they had a background in IT or law, and household income. We also included two attention check questions: one asking them to identify the name of a breach shown during the study (only for participants whose email address was part of at least one breach), and a generic attention check (see Appendix A.4). Finally, we showed participants a list of all breaches associated with their provided email addresses and links to resources on data breach recovery to help them process and act on this potentially new information.

3.1.2 Recruitment. We recruited participants via Prolific,[2] an online research platform similar to Amazon Mechanical Turk with more demographically diverse subjects [88], between August and October 2020. We recruited participants whose current residence is in the United States since some of the actions we are interested in examining (e.g., credit freezes) are US-specific. We balanced participants' age and gender distributions in data collection. After the first 171 participants, we realized and corrected a storage error that caused missing data in income and ratings for taken/intended actions. We note in Section 4 how we accounted for this in our analyses. Participants were compensated $2.50 for an average completion time of 13.37 minutes ($11.22/hour).

[2]https://prolific.co

3.1.3 Analyses. We collected data from 416 participants; three participants were excluded as they did not respond to any open-ended questions meaningfully, resulting in 413 participants in total. We based our sample size on our planned analyses: Bujang et al. [15] suggest n=500 or n=100 + 50 × #IVs as the minimum sample size for logistic regressions. For the linear regression (RQ4), G*Power suggests n=127 for detecting medium effects (f^2=.15), with α=.05, β=.80. With 413 participants (435 email-specific responses; 792 breach-specific responses) we met or exceeded these thresholds.

Ninety-seven percent of participants passed our generic attention check. Of the 302 participants who were shown at least one breach, only 55% passed the breach-specific attention check, whereas the rest chose "none of these" (42%) or a decoy option (3%). We reviewed open-ended responses from participants who failed this attention check, and all of them were detailed and insightful. We also did not find significant correlations between this attention check's performance and participants' breach-specific responses about awareness (chi-squared test, $\chi(1)$=.06, p=0.8), concern level (Mann Whitney test, W=58395, p=0.2), and whether they had taken action (chi-squared test, $\chi(1)$=.29, p=0.6). Thus, we did not exclude any of these participants as our findings suggest the question was not a reliable exclusion criterion.

Qualitative analysis. We analyzed participants' open-ended responses using inductive coding [109]. For Questions 7, 10, 14, 16, and 18, a primary coder created an initial codebook based on all responses. Multiple coders then iteratively improved the codebook. A second coder analyzed 20% of responses to each question to ensure high inter-rater reliability [70]. Cohen's κ were 0.89 (Q7), 0.73 (Q10), 0.74 (Q14), 0.81 (Q16), and 0.78 (Q18). We resolved all coding discrepancies through discussions. Appendix B includes the codebook, with common themes highlighted.

Statistical analysis. We conducted regressions to identify influential factors with respect to breach status (RQ1), awareness (RQ3), emotional response (RQ4) and behavioral response (RQ5). We included a random-intercept for individual participants to account for repeated observations between multiple breaches. However, for models corresponding to RQ1 the random effects were close to zero and caused a boundary singularity fit, so we conducted single-level regressions instead. For all models, we treated participant demographics (age, gender, education, occupational background) as control variables: we report a model's output with participant demographics when it has a significantly better fit than the model without; otherwise, we opt for the simpler model in reporting the results. We treated participants' responses of concern level on a 5-point Likert item as a continuous variable in our regressions, which has limitations, as we discuss in Section 3.4.

3.2 Method: Follow-up Survey

To investigate whether participants followed through with their self-reported intention as presented in the analysis of RQ5, we followed up with our participants six months after the main survey. The follow-up survey used the same infrastructure as the main survey and followed a similar analysis protocol, as we discuss below.

3.2.1 Survey Instrument. The follow-up survey focused on investigating whether participants followed through on their intentions to take action as reported in the main survey, covering 12 different actions. Compared to the main survey, we presented "reviewing credit reports" and "reviewing bank/credit card statements" as two separate actions since they require interactions with different entities. We also added "warning other people about this breach" as a new action since it was reported as a common reaction after data breaches in prior work [24, 133, 142]. Similarly to the main survey, we piloted the survey instrument with colleagues and students from our research labs, who were not involved in the project.

To shorten the time participants would need to fill out the survey, we split the actions depending on whether the action is breach-specific. Five actions apply to all breaches to the same degree: signing up for a breach notification service, signing up for an identity monitoring service, placing a credit freeze on credit reports, reviewing credit

reports for suspicious activity, and reviewing bank/credit card statements for suspicious activity. Seven actions are breach-specific: changing the password of the affected account, changing the password for other accounts that used the same password, enabling two-factor authentication, deleting the affected account, filing a complaint against the affected web service with a consumer protection agency, taking legal action against the affected web service, warning other people (e.g., friends and family members) about the breach. Due to this split, the survey consisted of two parts:

Part 1: Questions on actions applying to all breaches. After participants consented to participate in the study, they saw the questions relating to actions that apply to all breaches to the same degree. For each action, they were asked whether and when they had performed it since completing the main survey (Q30). The specific answer options include: "Yes – within a week;" "Yes – within a month;" "Yes – after a month or later;" "No – but I plan to do this soon;" "No – and I'm not planning to do this;" and "I already did this before the previous study." For participants who reported having signed up for a credit or identity monitoring service, we further asked whether they paid for the service and the specific brand (Q30a and Q30b). Next, we asked all participants to elaborate on the motivations for actions they took (Q31) and the impediments for actions they did not take (Q32). By asking about these actions only once, we significantly reduced the length of the questionnaire.

Part 2: Questions on breach-specific actions. After answering questions about actions applying to all breaches, participants were presented with the same (up to three) breaches they saw in the main survey. For each breach, we asked participants whether and when they had performed any of the breach-specific actions (Q33), as well as motivations and impediments for action (Q34 and Q35), using the same format as in Part 1. We ended the survey by asking participants to describe whether they have done anything else that we have not asked about (Q36).

3.2.2 Recruitment. All participants of the follow-up survey were among participants of the main survey. Specifically, we reached out to all 187 participants who were affected by at least one data breach according to results from our main survey but were not affected by the data recording error that resulted in missing data for taken/intended actions (cf. section 3.1.2). To encourage participation, we sent a private message to each eligible participant via Prolific, describing the follow-up survey's purpose and compensation and reminding them to check their Prolific dashboard as we released more slots. We started with a first batch of 15 participants as an additional piloting phase and then released the survey at full scale since no issues arose. Among these participants, 108 (58%) returned and completed the survey. Participants were compensated $2.50 for an average completion time of 10.14 minutes ($14.79 per hour).

3.2.3 Analyses. We analyzed the 108 complete responses for the follow-up survey, using a similar protocol as that of the main survey.

Qualitative analysis. Similar to the procedure used in the main survey, we used inductive coding [109] to analyze participants' open-ended responses to Questions 31, 32, 34, 35, and 36 in the follow-up survey. A primary coder created an initial codebook for all responses to these questions. A second coder analyzed 50% of each category of responses to ensure high inter-rater reliability. Cohen's κ were 0.78 (Q31), 0.71 (Q32), 0.84 (Q34), 0.80 (Q35), and 0.85 (Q36). Any disagreements were resolved through discussion among the coders.

Quantitative analysis. In the follow-up survey, we asked whether participants had taken the action since the main survey, with answer options starting with "yes" and "no" followed by more granular time ranges (Q30 and Q33). For each action, we ran logistic regressions with yes/no action as the dependent variable and the intention as the independent variable, in order to determine how reliably intention could serve as a proxy for predicting action. We excluded responses in which the participant selected "I did/do this already" or "This does not apply to me/I don't understand" in the main survey from the respective analyses.

Main Survey					Follow-up Survey	
Num. (%) W/ Breaches	Num. (%) W/o Breaches	Avg. (Med./Std.) Breaches	Total		Total	Avg. (Med./Std.) Breaches
139 (70%)	60 (30%)	4.49 (2/5.97)	**199**	**Men**	**39**	7.62 (7/5.65)
162 (76%)	50 (24%)	6.11 (4/6.28)	**212**	**Women**	**69**	8.32 (8/5.96)
1 (50%)	1 (50%)	11.00 (11/11.00)	**2**	**Non-Binary**	**0**	-
56 (73%)	21 (27%)	3.90 (2/5.15)	**77**	**18-24**	**10**	6.20 (3/6.63)
35 (69%)	16 (31%)	4.25 (2/4.90)	**51**	**25-29**	**5**	5.00 (2/5.05)
33 (79%)	9 (21%)	6.55 (3/8.72)	**42**	**30-34**	**5**	8.60 (10/6.95)
29 (59%)	20 (41%)	4.63 (1/7.05)	**49**	**35-39**	**8**	7.50 (5.5/6.57)
26 (58%)	19 (42%)	4.36 (2/5.04)	**45**	**40-44**	**7**	6.86 (7/3.19)
29 (91%)	3 (9%)	6.59 (4/6.05)	**32**	**45-49**	**15**	8.27 (6/6.52)
30 (77%)	9 (23%)	6.72 (6/6.16)	**39**	**50-54**	**17**	8.59 (7/5.50)
30 (88%)	4 (12%)	6.12 (5/4.82)	**34**	**54-59**	**19**	7.58 (7/5.25)
19 (70%)	8 (30%)	6.52 (3/6.85)	**27**	**60-64**	**11**	10.55 (13/5.99)
15 (88%)	2 (12%)	8.24 (8/6.06)	**17**	**65+**	**11**	9.36 (11/6.77)
0 (0%)	1 (100%)	0.00 (0/0.00)	**1**	**Some High School**	**0**	-
35 (76%)	11 (24%)	4.59 (3/4.61)	**46**	**High School or Equiv.**	**12**	6.08 (3.5/6.04)
70 (80%)	18 (20%)	5.67 (3/6.63)	**88**	**Some College**	**26**	8.08 (7/5.44)
14 (100%)	0 (0%)	8.07 (6/6.51)	**14**	**Associate (voc./occ.)**	**5**	5.2 (2/7.27)
19 (95%)	1 (5%)	6.10 (4/5.99)	**20**	**Associate (aca.)**	**6**	7.17 (4.5/6.97)
108 (77%)	32 (23%)	6.04 (4/6.56)	**140**	**Bachelor**	**39**	8 (7/5.55)
46 (55%)	37 (45%)	4.10 (2/5.68)	**83**	**Masters**	**19**	9.95 (10/5.71)
4 (80%)	1 (20%)	11.60 (13/7.71)	**5**	**Professional**	**1**	18.00 (18/-)
6 (38%)	10 (62%)	1.44 (0/2.26)	**16**	**Doctorate**	**0**	-
67 (55%)	55 (45%)	3.82 (1/6.30)	**122**	**IT Background**	**20**	7.35 (6.5/4.86)
224 (81%)	54 (19%)	5.91 (4/6.06)	**278**	**No IT Background**	**85**	7.99 (7/5.99)
11 (85%)	2 (15%)	8.00 (9/6.41)	**13**	**Prefer not to say**	**3**	15.00 (16/3.61)
14 (56%)	11 (44%)	5.80 (2/9.63)	**25**	**Law Background**	**3**	3.33 (2/3.22)
278 (74%)	96 (26%)	5.29 (3/5.93)	**374**	**No Law Background**	**101**	8.08 (7/5.81)
10 (71%)	4 (29%)	6.36 (5/6.25)	**14**	**Prefer not to say**	**4**	11.25 (11.5/6.80)
115 (68%)	55 (32%)	4.45 (2/6.21)	**170**	**No Data**	**1**	3.00 (3/-)
15 (94%)	1 (6%)	7.81 (4/8.59)	**16**	**<$15K**	**6**	4.17 (2/5.46)
20 (91%)	2 (9%)	6.77 (4/5.79)	**22**	**$15K-$25K**	**13**	8.615 (7/5.59)
26 (93%)	2 (7%)	5.89 (3/5.37)	**28**	**$25K-$35K**	**17**	7.12 (8/5.64)
19 (73%)	7 (27%)	4.58 (2/5.35)	**26**	**$35K-$50K**	**10**	7.00 (3/6.67)
40 (89%)	5 (11%)	8.04 (7/6.50)	**45**	**$50K-$75K**	**22**	8.77 (7/6.47)
28 (74%)	10 (26%)	6.95 (4/6.61)	**38**	**$75K-$100K**	**20**	9.90 (10/6.10)
22 (59%)	15 (41%)	4.05 (2/4.63)	**37**	**$100K-$150K**	**14**	7.857 (7.5/4.57)
13 (54%)	11 (46%)	3.92 (2/5.34)	**24**	**>$150K**	**5**	7.80 (7/5.54)
302 (73%)	**111 (27%)**	**5.36 (3/6.23)**	**413**	**Total**	**108**	**8.07 (7/5.83)**

Table 3. Participant demographics and breach status for the main survey (n = 413) and the follow-up survey (n = 108).

We further pre-processed some data to achieve homogeneity across the main and follow-up surveys. All questions about actions were breach-specific in the main survey, yet participants might report different intentions for the same action across different breaches. This requires us to consolidate the intention response across multiple breaches for comparisons with the follow-up survey responses. Specifically, we chose the value representing the highest likelihood to take action as the value for intention in the regression models (e.g., suppose a participant has seen two breaches in the main survey and has given the answers "not likely" and "very likely" regarding their intention to sign up for a breach notification service, "very likely" was the value for their intention). We decided on this procedure, speculating that if a person was very likely to perform an action in response to one breach, the intention and any respective outcomes likely would not be negated by lower intentions in response to a different breach. Additionally, the main survey combined reviewing credit reports and financial statements as one action, whereas in the follow-up survey they were separated. For the purpose of running regressions, in the follow-up survey we counted it as having followed through with the intention if the participant reported having performed any of the two actions.

3.3 Samples

Participant profile for the main survey. Table 3 summarizes the demographics and breach status of our 413 participants from the main study, alongside the demographics form the follow-up survey to allow for easy

comparison. Our participants were almost evenly distributed between men and women but skewed educated and younger. Regarding occupational background, 122 (30%) described having a background in information technology; 25 (6%) in law.

In total, participants provided 435 email addresses. Among these email accounts, 421 (97%) were solely owned by the participant, and ten were shared with someone else. Four were either someone else's account or a made-up address for the study, and so were removed from the data. Participants whose initial email address was not exposed in any breach could scan another: 393 participants (95%) scanned only one email address, 18 scanned two addresses, and only two scanned three addresses.

For the 431 owned or shared email accounts, we further asked participants how long they had been using the email account, how frequently they checked it, and what they primarily used it for. The majority of email accounts were used for an extended period (mean: 8.75 years, median: 8). Most (81%) were checked daily; the rest were checked less frequently (14% weekly, 4% monthly, and 1% yearly). Participants reported multiple uses for their email address (mean: 2.74, median: 3): 74% were used for personal correspondence, followed by signing up for medium-sensitive accounts like social media (68%), signing up for sensitive accounts like banking (51%), signing up for low-value accounts (49%), and professional correspondence (32%).

Participant profile for the follow-up survey. Table 3 also gives an overview of the 108 participants of the follow-up survey. The gender distribution in the follow-up survey is considerably skewed: 69 (64%) participants identified as women and 39 (36%) identified as men. The skew towards younger participants in the main survey has now shifted, with a majority of 62 (57%) being 45 years or older. The portion of participants with a background in technology (20; 19%) and law (3; 3%) dropped to two-thirds and half the portions of the main survey respectively. When asked whether they recalled the main survey, the vast majority of participants (88; 82%) recalled taking the main survey, 11 (10%) participants were not sure, and nine (8%) participants did not recall the main survey.

Overview of breaches. We observed 189 unique breaches across 431 email addresses queried against HIBP. The majority (302; 70%) of email addresses, or 73% of participants, were exposed in one or more breaches. The average number of breaches per email address was 5.12 (median: 3, sd: 6.21, max: 46), or 5.36 per participant (median: 3, sd: 6.23). The number of breaches per email address formed a long-tail distribution: 34% of email addresses appeared in 1 to 5 breaches, and only 2% were associated with 21 or more breaches.

For the 189 unique breaches, we examined their date, the total amount of breached accounts, and the types of compromised data according to HIBP. The majority (69%) of breaches occurred in 2015–2019; 15 breaches occurred in 2020. The average number of breached accounts captured by HIBP was 46.52m (median: 4.79m; sd: 125m), indicating a distribution skewed by several large breaches (max: 772.90m). Sixty-six different data types were leaked in our sample's breaches. The average number of leaked data types per breach was 4.86, and the maximum was 20 (median: 4, sd: 2.58). Aside from participants' email addresses (which were present in all breaches as HIBP uses them as references), the other commonly breached data types included passwords (162, 86%), usernames (110, 58%), IP addresses (82, 43%), names (74, 39%), and dates of birth (47, 25%). The frequency distribution of data types in our sample's breaches falls off steeply (see Figure 2), suggesting a broad range of leaked data types with a much smaller set of commonly leaked data.

We used Cisco's website content taxonomy[3] for cross-referencing each breached site's industry, excluding 25 (13%) non-applicable cases.[4] Gaming companies had the highest representation in our sample (40, 21%). Other represented industries included general business (17, 9%), computers/Internet (16, 8%), shopping (10, 5%), and online communities (10, 5%). We used Alexa's ranking of global websites[5] as of October 14, 2020 as a proxy for

[3]https://talosintelligence.com/categories

[4]These breaches were spam lists or aggregate credential stuffing lists, or the breached site was no longer active.

[5]https://alexa.com/topsites

a breached site's popularity.[6] Excluding 33 organizations with missing data, the average ranking was 650.73k (median: 24.85k, sd: 1,768k). Nineteen organizations appeared in the top 1k list, indicating that while the majority of organizations in our sample were not mainstream, a few were relatively well-known.

3.4 Limitations

First, both surveys rely on participants' self-reported data, which could be prone to recall and social desirability biases. Prior work has shown that self-reported data in security user studies can translate to real-world environments; discrepancies may arise when survey respondents are asked to notice and act on minor details of experimental manipulations [100] — this condition, however, does not apply to our research.

There are limitations associated with using HIBP as the source of data breaches. HIBP's API does not return breaches marked sensitive such as those involving adult sites. Accessing these breaches requires sending a confirmation message to participant-provided email addresses for ownership verification. We decided not to do this as it may suggest to participants that we store their email addresses even though we did not. In addition, our research only covers data breaches involving email addresses, which do not represent all breaches (e.g., only 9% of all breaches in 2017-2021 recorded by the Identity Theft Resource Center included email/password [51]). Relatedly, the email-focused nature of these breaches means it is difficult to track whether and how breached organizations in our sample notified affected individuals and how that impacts consumer reactions, as existing breach notification databases mostly document letter-based notifications [141]. Future research can look into breaches that expose a broader range of data types and consider organizations' handling of breaches when feasible.

For the Likert responses of concern level in the main survey, we considered several options for how they should be treated in the analyses: ordinal, nominal, or continuous variables. Treating concern as an ordinal variable would introduce square and cubit effects into the model — these effects are difficult to interpret and inconsistent with the scale. Treating concern as a nominal variable would lose information about the scale's ordering and prevent comparisons across all levels (e.g., with "not at all concerned" as the baseline, the regression would not describe the difference when moving up or down the scale between "slightly concerned" and "extremely concerned"). Treating concern as a continuous variable would require a more cautious interpretation of the p-values in the analysis, and it assumes equal differences between the scale items. After discussions with our institution's statistical consulting service, we followed their advice and decided to treat concern as a continuous variable. While this comes with the limitations mentioned above, it also allows a more straightforward and meaningful interpretation of results, which we prioritize to make the results more accessible.

For the follow-up survey, we decided to shorten the questionnaire based on feedback from pilot testing. While this significantly reduced the survey's completion time and provided a more straightforward structure, it rendered the analysis more complex due to the additional steps required to homogenize the data between the original and follow-up measurements (cf. Section 3.2.3). Moreover, the sample size for the follow-up survey (n=104) is much smaller than that for the main survey (n=413) since we could only invite part of the main survey participants back due to our data recording error, and about half of the participants who received our invitation did not return. The regression analyses for the follow-up survey are underpowered according to Bujang et al.'s suggested thresholds [15] and our regression results should be interpreted with caution. We further discuss this in Section 6.

[6]We used rankings at the time of analysis rather than historic ranking (i.e., the ranking when the breach occurred) because (1) Alexa only provides ranking data for the last four years; and (2) we anticipate that the current ranking would better reflect participants' impression of the organization's popularity at the time when they took our study.

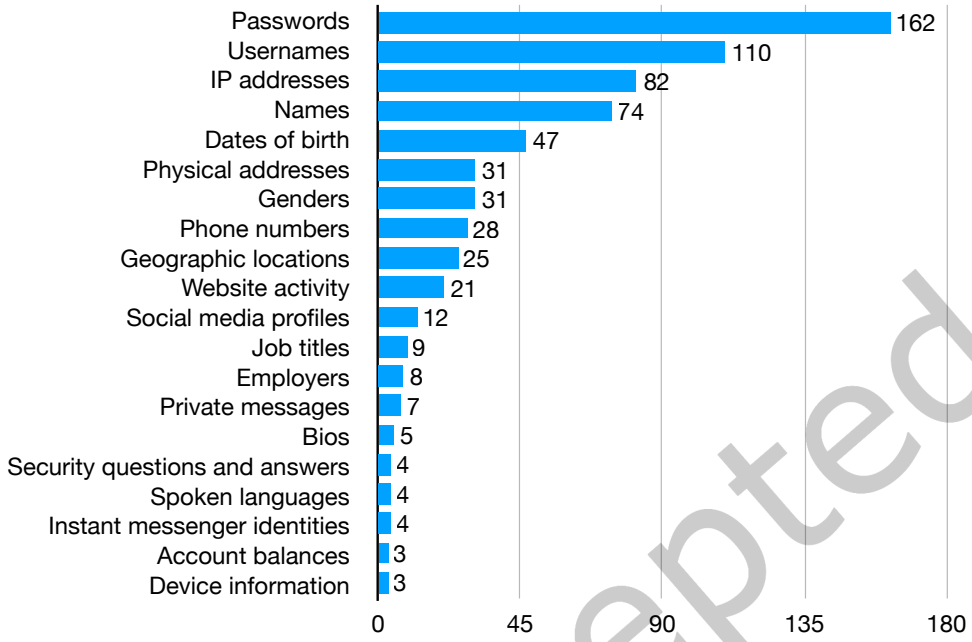


Fig. 2. Frequency of the leaked data types for 189 breaches, excluding email address (appears in all breaches). 44 other types occurring twice or fewer.

4 Results: Main Survey

4.1 RQ1: Likelihood of Breaches

We conducted a logistic regression on whether an email address had been exposed in data breaches in relation to the email account's age, frequency of being checked, and purpose of use. Results in Table 4 show that an email address was significantly more likely to be exposed in data breaches as the account's age in years increased (OR_{age}=1.35, p<.001), as it was checked daily instead of weekly (OR_{daily}^{weekly}=2.30, p=.03), and as it was used for personal correspondence (OR_{yes}^{no}=2.13, p=.02). Additionally, the significant intercept indicates that an email address was significantly unlikely to be associated with any breach if the email account was just created, checked weekly, and not used for any correspondence or account creation purposes ($OR_{intercept}$=0.14, p=.002). Essentially, the less frequently used and newer an email address is, the less likely it is to be exposed in a breach.

We further conducted a quasi-Poisson regression on the number of breaches per email address with the same independent variables as above. We chose quasi-Poisson regression because the dependent variable is count data with a skewed distribution [139]. Results in Table 5 show how the number of breaches increases with an email account's age: for every one year of increase in age, the expected number of breaches increases by a factor of $exp(0.08) = 1.08$ (p<.001). In other words, the number of breaches increases 8% per year of use, compounding yearly (see Figure 3). A possible explanation is that the older an email address is, the more it has been used for account registrations, which increases its presence on the Internet as well as risks of exposure when a data breach occurs. The significant intercept in Table 5 confirms this finding: a new and rarely used email address is less likely to be affected by breaches. Furthermore, the number of breaches per email address differed among age groups: compared to young adults (18-34), the number of breaches decreases by a factor of $exp(-0.29) = 0.75$

Table 4. Logistic regression for breach status of an email address (leaked vs. not leaked).

	Est.	OR	95% CI	p-value
(Intercept)	−1.95	0.14	[0.04, 0.49]	.002
Freq. Checked daily (vs. weekly)	0.83	2.30	[1.07, 4.99]	.03
Prof. Corr. yes (vs. no)	−0.02	0.98	[0.51, 1.87]	.94
Pers. Corr. yes (vs. no)	0.76	2.13	[1.13, 4.03]	.02
Acct. Creat. yes (vs. no)	0.31	1.36	[0.60, 3.07]	.46
Email age years	0.30	1.35	[1.26, 1.46]	< .001
Age: 35-54 (vs. 18-34)	−0.51	0.60	[0.29, 1.23]	.16
Age: 55+ (vs. 18-34)	−0.60	0.55	[0.27, 1.10]	.09
Gender: men (vs. women)	−0.24	0.79	[0.43, 1.45]	0.45
Edu.: =Bach. (vs. <Bach.)	0.25	1.28	[0.65, 2.53]	0.48
Edu.: >Bach. (vs. <Bach.)	−0.62	0.54	[0.25, 1.16]	.11
Occu.: IT/law yes (vs. no)	−0.51	0.60	[0.31, 1.17]	.14

Table 5. Quasi-poisson regression regarding the number of breaches per email address.

	Est.	Exp (Est.)	SE	p-value
(Intercept)	0.67	1.94	0.26	.01
Freq. Checked daily (vs. weekly)	0.36	1.43	0.19	.06
Prof. Corr. yes (vs. no)	−0.11	0.89	0.12	.33
Pers. Corr. yes (vs. no)	0.29	1.34	0.15	.06
Acct. Creat. yes (vs. no)	−0.18	0.83	0.15	.22
Email age years	0.08	1.08	0.01	< .001
Age: 35-54 (vs. 18-34)	−0.29	0.75	0.14	.045
Age: 55+ (vs. 18-34)	−0.35	0.71	0.14	.02
Gender: men (vs. women)	−0.18	0.84	0.12	.13
Edu.: =Bach. (vs. <Bach.)	0.17	1.18	0.12	.18
Edu.: >Bach. (vs. <Bach.)	−0.17	0.84	0.16	.29
Occu.: IT/law yes (vs. no)	−0.05	0.95	0.14	.70

(p=.045) for middle-aged adults (35-54) and by a factor of $exp(-0.35) = 0.71$ (p=.02) for older adults (55+).

RQ1: What factors influence the likelihood that an email address is involved in a data breach? Our results suggest that an email account's age, checking frequency, and purpose of use are significantly correlated with the email address's presence in a breach. Both models capture email age's influences: for each year of increase, the email address is 1.35x more likely to be part of a breach or gains 1.08x more breaches than the previous year. Conversely, the significant intercept in both models suggests that a new and rarely used email address is less likely to be involved in a breach. While these results are somewhat intuitive, they indicate the pervasiveness of data breaches: most email addresses queried in our study had appeared in one or more breaches even though they were only used in ordinary ways.

4.2 RQ2: Perceived Causes and Impacts of Being Affected by Breaches

We asked participants to speculate why or why not their email address was part of a data breach and name any experienced impacts or anticipated future impacts from a specific breach.

Perceived reasons for being affected by breaches. We analyzed 302 open-ended responses to Question 10 in which participants speculated why their email address was exposed in one or more data breaches. The most common speculation, cited in 159 (53%) responses, was that it was due to their own email-related practices. Specifically, 70 (23%) mentioned using the email address to sign up for many different sites (e.g., *"it's on the website of every*

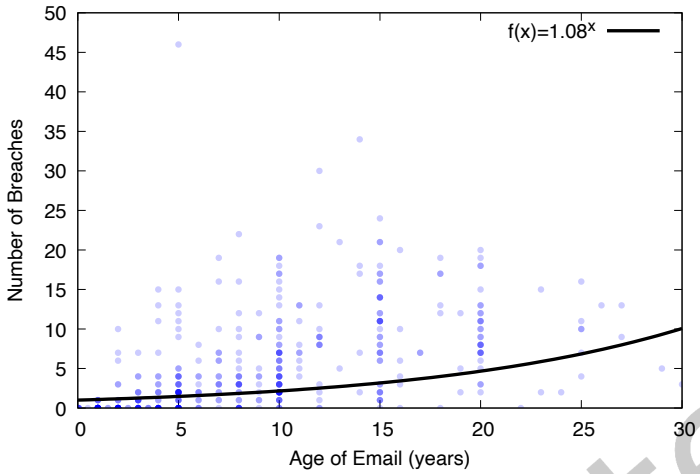


Fig. 3. Number of breaches vs. age of email address (years); curve represents an 8% increase in number of breaches per year as estimated by the quasi-Poisson regression.

business I have an online relationship with"). Another 31 (10%) mentioned the email's age as a relevant factor, saying it had been used for a long time. 23 (8%) expressed that breaches were inevitable, especially for an old or widely-used email address (e.g., *"there are a lot of companies or organizations that have my email [address] and chances are one of them is going to get hacked"*). Furthermore, in 31 (10%) cases, participants mentioned using the email address to sign up for seemingly sketchy websites, sometimes with a clear intention to do so despite knowing that the website might be insecure.

Participants mentioned other insecure behaviors as potential reasons for being affected by a breach in 31 (10%) cases. In 13 responses, participants referred to password-related behaviors, such as using simple passwords, reusing a password across accounts, or not changing passwords frequently. Incautious clicking behavior was mentioned five times (e.g., *"because I was not careful with what emails I clicked"*). Other participants indicated their exposure to breaches was due to infrequent monitoring of the email account, easily guessed answers for security questions, or forgetting to log out of the email account. While these are indeed insecure behaviors, password choices do not impact one's likelihood of being involved in a breach; they impact a breach's consequences by increasing the possibility of account hijacking due to credential stuffing. Similarly, clicking on untrustworthy links may make the email address appear in spam lists, which will be reported by HIBP if found on the public web. However, this action on its own does not increase one's vulnerability to breaches.

Participants in only 42 (14%) of all responses accurately attributed the cause of being affected by a breach to external factors unrelated to their behaviors. In 26 (9%) cases, participants blamed lax security measures by the breached site (e.g., *"these companies did not try hard enough to keep information private"*). Sixteen (5%) blamed bad actors such as hackers and scammers targeting the breached site (e.g., *"hackers are devious devils and learn to adapt faster than organizations can protect users"*). Another 15 (5%) suspected their email address was sold by the breached site or a third party. Nine participants incorrectly placed blame on their email provider's security (e.g., *"I feel like Hotmail has poor security and cannot block as many spam emails compared to Gmail"*).

Perceived reasons for not being affected by breaches. Question 7 asked participants to speculate why their email address was *not* involved in any data breach. Among the 136 provided responses, 78 (57%) mentioned cautious email practices. Specifically, 31 (23%) reported using their email address to sign up for trusted sites only, sometimes

with careful examination of the website (e.g., *"I try as much as possible to scrutinize websites before dropping any of my details"*). Eighteen (13%) mentioned that their email address was relatively new or did not get used much, which is supported by our regression results in Section 4.1. Ten mentioned limiting the email to specific purposes, such as correspondence with friends and family members only.

Eight participants described using multiple email accounts for different purposes, e.g., using one email address for correspondence exclusively and another for account registration on sites to which they do not attach much value (i.e., "low-value" sites). Such behavior would likely reduce the likelihood of breaches involving high-value email addresses. However, low-value email addresses that are commonly used for account registration still face real impacts of breaches such as account hijacking.

Twenty-one (15%) participants cited their security practices as reasons for not being affected. Nine participants mentioned their password practices, such as using strong/unique passwords and changing passwords regularly. Less frequently mentioned were two-factor authentication, anti-virus, firewall, and VPN. None of these behaviors are likely to prevent data breaches despite potentially having other positive security outcomes.

Experienced and anticipated impacts of data breaches. Participants with at least one breach were asked to describe their experienced or potential impacts for a given breach (Question 16). Of the 792 responses, more than half assessed the breach's impact as none (343, 43%) or very little (85, 11%); another 77 (10%) were unsure. Only 19 (4%) breaches were perceived as having a large impact. In 135 (17%) cases, participants described emotional feelings without naming concrete impacts, such as *"no impact, just rage."*

In 149 (19%) instances, participants described specific experienced impacts or anticipated future impacts. The most prevalent was an increase in spam emails and text messages. Some participants reported scam phone calls, and others anticipated identity theft as a potential impact (e.g., *"I suppose now that someone has all that information about me they could impersonate me, open credit lines in my name, scam my family and friends"*). Participants who had experienced adverse events described emotional stress and resulting behavioral changes, such as avoiding phone calls due to frequent scams or frequently checking emails for suspicious activities after account compromises.

Notably, participants with and without experienced impacts differed in assessing the impact's severity. Most participants who described anticipated impacts but had not experienced them did not foresee real consequences (e.g., *"the only things that [would] really happen is … scammers … occasionally attempt to access some of my older accounts that hold no sensitive information"*). This finding underlines that participants' perception of impacts after being affected by breaches largely depends on individual circumstances. Prior work [142, 143] has similarly shown that people don't adopt secure behaviors until experiencing actual harm.

RQ2: What do participants perceive as the causes of being involved in data breaches and related impacts, and to what extent do their perceptions align with reality? Our results indicate that relatively few participants (42 out of 302, 14%) correctly attributed the cause of their victimhood to external factors such as the breached site and hackers. Instead, most participants referred to their insecure behaviors related to email, passwords, etc., in explaining why their email address appeared in a breach. Most participants reported little to no experienced or anticipated impacts. When participants named concrete consequences, they mostly referred to spam and identity theft, though the perceived severity varied substantially.

4.3 RQ3: Awareness of Breaches

Among the 792 breach-specific responses, 590 (74%) reported unawareness of being affected by the breach before our study. Only 143 (18%) reported prior awareness, and the other 8% were unsure. Participants who were previously aware of the breach mostly learned about it from the breached site (45, 31%) or third-party notification services (45, 31%). Less common sources included news media (17, 12%), credit/identity monitoring services (14,

Table 6. Logistic regression regarding prior breach awareness.

	Est.	OR	95% CI	p-value
(Intercept)	−4.24	0.01	[0.002, 0.09]	< .001
Freq. Checked daily (vs. weekly)	0.31	1.37	[0.45, 4.16]	.58
Prof. Corr. yes (vs. no)	−0.06	0.94	[0.45, 1.98]	.88
Pers. Corr. yes (vs. no)	0.22	1.25	[0.50, 3.10]	.63
Acct. Creat. yes (vs. no)	0.77	2.15	[0.70, 6.63]	.18
Email age years	0.04	1.04	[0.98, 1.11]	.17
Breach age years	0.20	1.22	[1.09, 1.35]	< .001
Age: 35-54 (vs. 18-34)	−0.41	0.66	[0.27, 1.61]	.36
Age: 55+ (vs. 18-34)	−0.94	0.39	[0.15, 1.00]	.049
Gender: men (vs. women)	0.74	2.09	[1.00, 4.37]	.049
Edu.: =Bach. (vs. <Bach.)	−0.79	0.45	[0.20, 1.00]	.051
Edu.: >Bach. (vs. <Bach.)	−0.18	0.84	[0.31, 2.22]	.72
Occu.: IT/law yes (vs. no)	0.50	1.65	[0.72, 3.77]	.23

10%), bank or credit card companies (3, 2%), experiencing adverse events (3, 2%), and someone else (3, 2%). In nine instances, participants could not remember how they learned about the breach.

We ran a mixed-effect logistic regression to identify factors that might impact awareness (excluding "unsure" responses), including the same email-related factors from Table 4 as independent variables. Additionally, we included breach age (i.e., the time lapse between a breach's occurrence and the participant taking our study), hypothesizing that participants are more likely to recall and report awareness of recent breaches.

Results in Table 6 show a significant intercept, indicating that participants were more likely to be unaware of a breach if they have a newer email address and the breach just occurred ($OR_{intercept}$=0.01, p<.001). Participants were also significantly more likely to be aware of a breach as the breach's age in years increased (OR_{breach_age}=1.22, p<.001). Older participants were less likely to be aware of breaches than young participants (OR_{55+}^{18-34}=0.39, p=.049), and men were more likely to be aware of a breach than women in our sample (OR_{men}^{women}=2.09, p=.049), though p-values in both cases are close to 0.05. These findings align with prior work in which adopting protective behaviors differed by age [62] and gender [114, 143]. Other demographic variables and email-related factors are not significantly correlated with prior awareness.

RQ3: What factors influence participants' awareness of data breaches that affected them? Participants were unaware of 74% of the breaches presented in our study, suggesting that current methods of informing consumers about data breaches might be ineffective. Prior awareness primarily came from interactions with the breached company

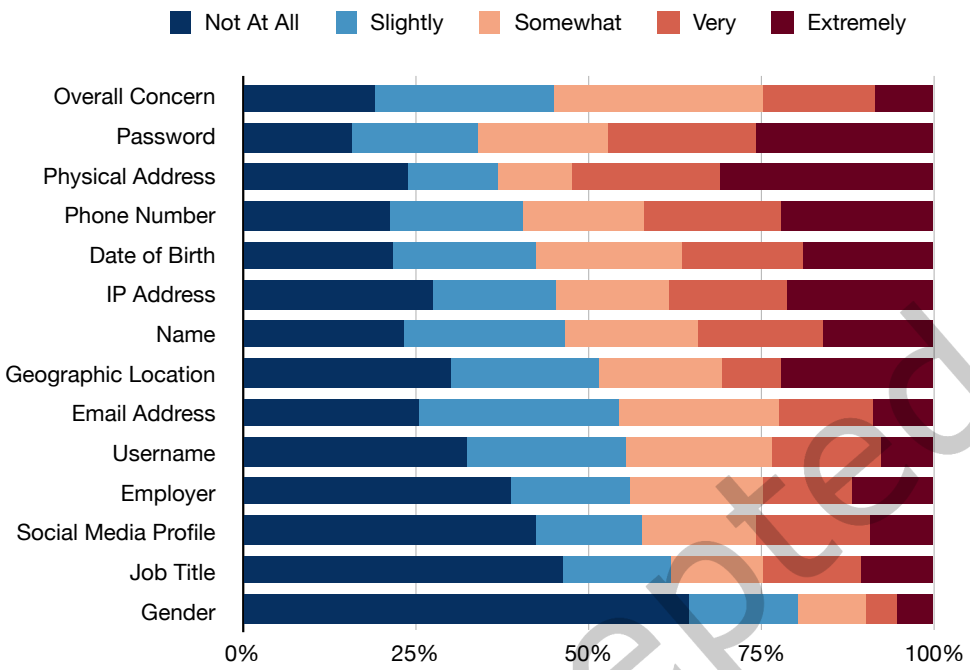


Fig. 4. Overall concern (Question 15) about the breach and levels of concern for the 13 most commonly leaked information types in our sample breaches (Question 17).

or third-party notification services. Notably, participants were significantly more likely to be aware of older breaches. A longer time-lapse might provide participants with more opportunities to learn about the breach, and once aware, participants' memory of the breach does not seem to fade away.

4.4 RQ4: Emotional Response and Concerns towards Breaches

Participants indicated their concern using a 5-point Likert item for each shown breach (Question 15) and for each data type leaked in a breach (Question 17). We also asked participants to describe their feelings after learning about the breach (Question 14, open-ended).

Quantitative ratings of concern level. Among 792 breach-specific responses, the median concern level regarding the breach was "somewhat concerned." Less than half reported either no concern (151, 19%) or being very/extremely concerned (197, 25% combined). Figure 4 shows concern levels for commonly leaked data types. Participants were most concerned about leaks of physical address (52% very/extremely), passwords (47% very/extremely), and phone number (42% very/extremely). Other leaked data types that participants felt less concerned about were employer information (38% not at all), social media profile (42% not at all), job title (46% not at all), and gender (65% not at all).

We sought to identify factors that might impact concern level through a mixed-effect linear regression on overall concern Likert responses. We included email address-related factors and prior awareness as independent variables, hypothesizing that participants would be more concerned about frequently used email addresses or if they had not been aware of a breach. We also included the number of breached data types and the breach status of data types for which more than 50% of responses were "somewhat concerned" or above in Figure 4, namely

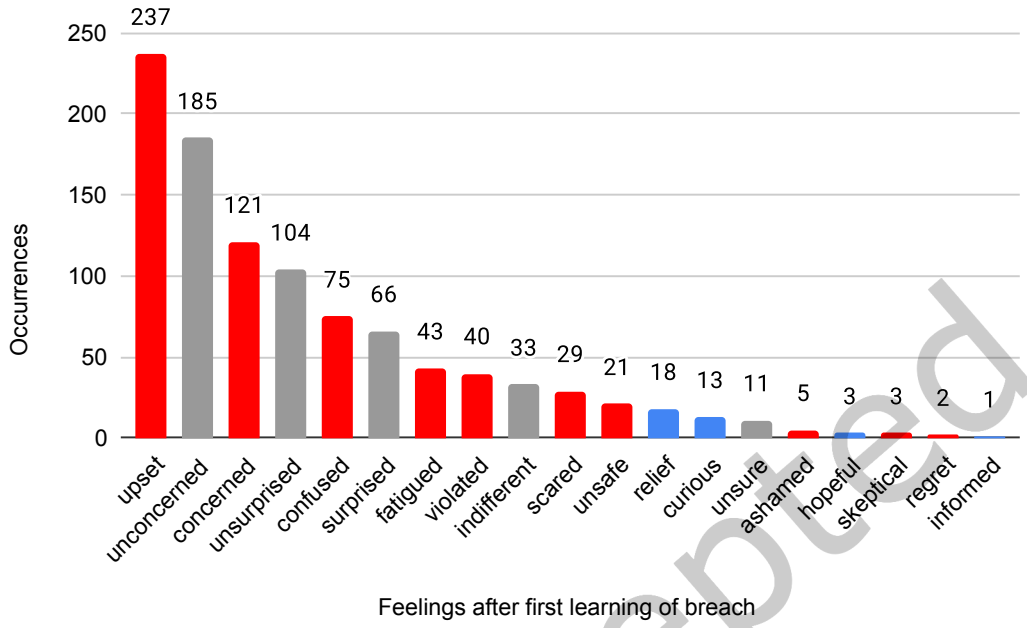


Fig. 5. Code frequencies for feelings after first learning about a breach (n = 792); red bars indicate negative feelings, gray neutral, blue positive, according to Emolex ratings [82].

password, physical address, phone number, date of birth, IP address, and name.[7] We hypothesized that as the amount or sensitivity of leaked data types increases, the concern level would increase. Additionally, we included the breaches' age, hypothesizing that participants might be more concerned about more recent breaches since these breaches would likely involve data that is still relevant to them.

The regression results do not reveal any significant factors impacting overall concern except the intercept ($b_{intercept}$=2.52, SE=.31, p<.001), indicating that participants likely default to between "slightly concerned" and "somewhat concerned." The model's f^2 = 0.03 indicates a small effect size. The absence of significant correlators for concern is likely due to the fact that sensitive data types (e.g., financial information and social security numbers that are known to trigger more concern) are underrepresented in our sample's breaches (see Figure 2). Even relatively sensitive data types in our sample still had a fair number of "not at all/slightly concerned" responses.

Various emotions in qualitative responses. Figure 5 shows the wide range of emotions reflected in participants' open-ended responses about their feelings after learning of a breach affecting them. In 237 (30%) cases, participants reported feeling upset (including annoyed, frustrated, mad, and angry), mostly toward the breached site. The negative emotion came from not having been properly informed (e.g., *"I was very disappointed . . . they hid the fact that there was a data breach from everyone for three months"*), the organization's poor security measures (e.g., *"don't run an entirely online business if you can't do basic security"*), or violation of consumers' trust (e.g., *"I joined this site to read a story my granddaughter had written and thought it was completely safe"*). These emotions align with the "risk as feelings" theory, which highlights that people may experience dread and outrage in comprehending risks [116].

[7]Email address was not included because it was exposed in all breaches in our sample, making no positive vs. negative cases.

Mirroring the Likert responses, feeling unconcerned about a breach was common (185, 23%). Many participants believed that the exposed data was not sensitive (e.g., *"I had only used the free version of that site, so I had not entered any payment information"*). Others were unconcerned because they rarely interacted with nor knew the breached site (e.g., *"I don't even know what this site is, so I don't think that them having my info . . . is a huge deal"*). Some were unconcerned due to confidence in their security habits, including regularly changing passwords (25), avoiding password reuse (10), and enabling 2FA (4). A few participants were unconcerned due to a lack of experienced impacts (e.g., *"I'm not especially worried because I haven't detected any suspicious activity"*) or the thought that they were less likely to be affected than others (e.g., *"I feel like a drop in the bucket since there were 711 million emails affected"*).

Participants in 104 (13%) responses reported feeling unsurprised whereas 66 (8%) reported feeling surprised. Unsurprised participants explained that they never trusted the breached site or already knew about the breach. Conversely, surprised participants stated that they had never used the breached site's service or trusted the organization.

In another 75 (9%) of cases, participants expressed confusion due to unfamiliarity with the breached site or not remembering having an account. Other prominent emotions included fatigued (43, 5%), violated (40, 5%), indifferent (33, 4%), scared (29, 4%), unsafe (18, 2%), relieved (18, 2%), or curious about why the breach happened (13, 2%). Those who expressed fatigue stressed that breaches were inevitable (e.g., *"It's the internet and things WILL be leaked somehow, either by hackers or by incompetence at the company that is holding your information anyhow"*). This attitude is akin to the "digital resignation" phenomenon [32]: many people's inaction in the face of privacy infringements is not necessarily because they do not care, but because they are resigned and convinced that surveillance is inescapable. Positive emotions like relief were rare. Participants were relieved when sensitive data like financial information was not involved or that they were now aware of the breach and could take proper action.

RQ4: What are participants' emotional responses to data breaches that affected them? While some leaked data types (e.g., password, physical address, and phone number) triggered more concerns, overall participants reported low concern about data breaches: 56% were slight or somewhat concerned, and 19% were not at all concerned. However, participants expressed a rich set of (mostly negative) emotions beyond concerns, such as feeling upset with the breached site and feeling fatigued by the sheer number of data breaches nowadays.

4.5 RQ5: Behavioral Intention to Breaches

Participants were already aware of 143 breaches before our study. For these breaches, we further asked if they had taken any action in response (Questions 18). From participants' open-ended responses, the most common action taken was to change passwords (87; 61%). Fifteen specified that they changed the password for the account at the breached site, and 27 mentioned changing the password across multiple accounts that might use the leaked password. Five further mentioned changing their email account's password; this could be due to a misconception that their email account, not the account with the breached site, was compromised. Participants also described other password-related practices triggered by the breach, such as using unique passwords, using a password manager, and making passwords more complicated.

For actions related to participants' accounts with the breached site, participants in 18 (13%) responses mentioned deleting or deactivating their accounts, and one mentioned reviewing accounts on other websites and deleting them as needed. Five mentioned enabling 2FA for the account with the breached site, for other accounts, or for their email account. Four reported checking the breached site's account to see if it stored any sensitive data or if there had been any suspicious activity. In 31 (22%) cases, participants reported doing nothing in reaction; the percentage was lower than that in Ponemon's 2014 survey (32%) [53], but still substantial.

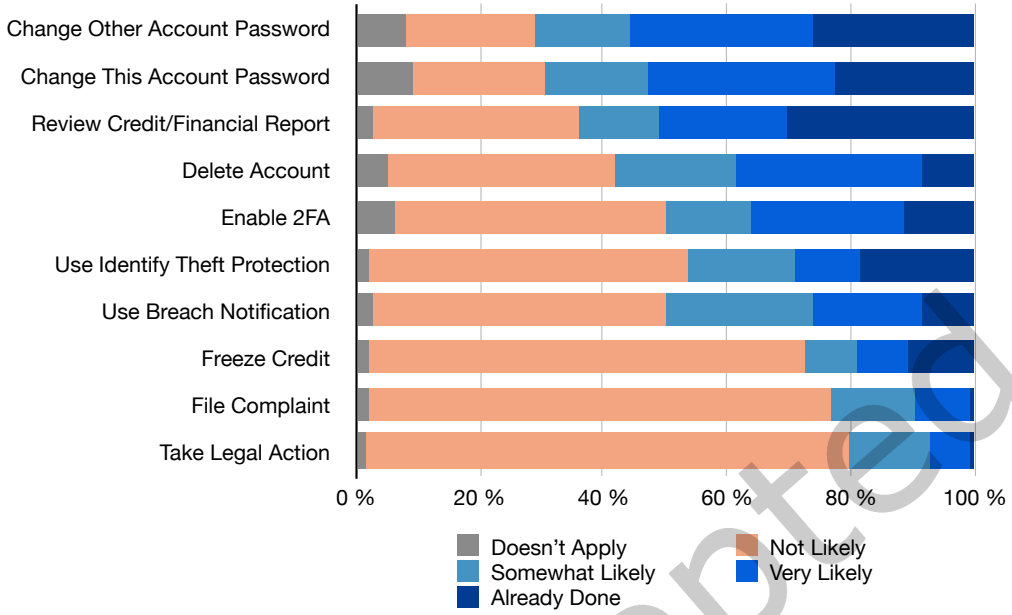


Fig. 6. Intention to take actions within the next 30 days.

Additionally, we asked all participants with at least one breach to indicate, for each breach, how likely they were to initiate ten provided actions within the next 30 days or whether they had taken action already. Specifically, we asked about the following actions:

- *Change the Password for the Affected Account.* Whether participants changed the password for the account at the service that experienced the specific breach in question.
- *Change Reused Passwords for Other Accounts.* In extension to the password at the service directly affected by the breach, this action refers to accounts at different services that reuse the same password.
- *Delete Account.* Whether participants deleted or deactivated the account at the service that experienced the specific breach in question.
- *Enable Two-Factor Authentication.* Whether participants enabled two-factor authentication (2FA) at the service that experienced the specific breach in question.
- *File a Complaint.* Whether the participant filed a complaint with a consumer protection agency or any other regulatory entity to receive compensation for damages resulting from the breach.
- *Place a Credit Freeze.* Whether the participant placed a credit freeze on their credit reports at the three major credit bureaus (or credit reporting agencies) in the US—Experian, Equifax, and TransUnion.
- *Review Credit Reports and/or Financial Statements.* Whether the participant reviewed credit reports and/or bank and credit card statements for fraudulent activities.
- *Take Legal Action.* Whether the participant took legal action against the service affected by the specific breach in question.
- *Sign Up for Breach Notifications.* Whether the participant signed up for a breach notification service (e.g., Have I Been Pwned, Firefox Monitor).
- *Sign Up for Credit/Identity Monitoring.* Whether the participant signed up for a credit monitoring or identity theft protection service (e.g., LifeLock, Identity Guard, Credit Karma).

Table 7. Logistic regression on taking action in the main survey.

	Est.	OR	95% CI	p-value
(Intercept)	−3.27	0.04	[0.002, 0.61]	.02
Awareness yes (vs. no)	5.97	390.48	[45.72, 3334.79]	< 0.001
Breach age years	−0.03	0.97	[0.77, 1.21]	.77
Num. of types numeric	.12	1.13	[0.85, 1.50]	.39
Password yes (vs. no)	−0.18	0.84	[0.18, 3.79]	.82
Physical Addr. yes (vs. no)	−0.26	0.77	[0.16, 3.71]	.75
Phone Num. yes (vs. no)	−0.29	0.75	[0.19, 3.02]	.69
Date of birth yes (vs. no)	−0.24	0.79	[0.17, 3.62]	.76
IP Addr. yes (vs. no)	−0.20	0.82	[0.26, 2.64]	.74
Name yes (vs. no)	−0.19	0.83	[0.21, 3.22]	.79
Concern numeric	0.80	2.22	[1.28, 3.86]	.005

We only include 500 breach-specific responses in the following analysis due to a data storage issue, excluding incomplete responses. Figure 6 shows the results. Of the ten provided actions, changing the password for the breached site's account or other accounts was the most popular, receiving more than half of likely/already done responses. "Review credit reports and/or financial statements" had the highest percentage of already done (30%). By contrast, most participants selected "not likely" for four actions — "use a credit/identity monitoring service," "place a credit freeze on my credit reports," "file a complaint with a consumer protection agency," and "take legal action against the breached site." This finding is understandable given that most leaked data types such as email addresses and passwords are considered "non-sensitive records" according to ITRC's definition [52].

We sought to understand factors that would impact the likelihood of having taken any of the ten provided actions through a mixed-effect logistic regression. For independent variables, we discarded variables related to email habits since many of the listed actions were unrelated to one's email account. We kept all other independent variables from the concern regression model, namely prior awareness, the breach's age, the number of breached data types, and the breach status of six data types with relatively high concern levels. We further included overall concern Likert responses as an independent variable. Results in Table 7 show a significant intercept, indicating that participants were likely to default to inaction with no leaked data and no prior awareness or concern ($OR_{intercept}$=0.04, p=.02). Being aware of a breach significantly increased the likelihood of having taken any of the listed actions (OR^{no}_{yes}=390.48, p<.001). This is unsurprising given that participants who were unaware of being affected had little motivation to engage in protective measures. Additionally, more concern was significantly correlated with a higher likelihood of having taken action: for a one-unit increase of concern on the 5-point Likert item, the odds of having taken action increase by 2.22 ($OR_{concern}$=2.22, p=.005).

RQ5: What factors influence participants' intention to take action in response to data breaches that affected them? Participants' intention to act varies among protective measures: they were more amenable to changing passwords and checking credit reports/financial statements than other actions. The regression results reveal that awareness and concern are significantly correlated with the likelihood of taking action, while other factors such as the leaked data types do not impact the outcome. Our findings suggest that to motivate consumers to react to breaches, they must first be aware that the breach occurred and feel concerned enough to invest in mitigation efforts.

5 Results: Follow-up Survey

5.1 RQ6: Following Through on Intention

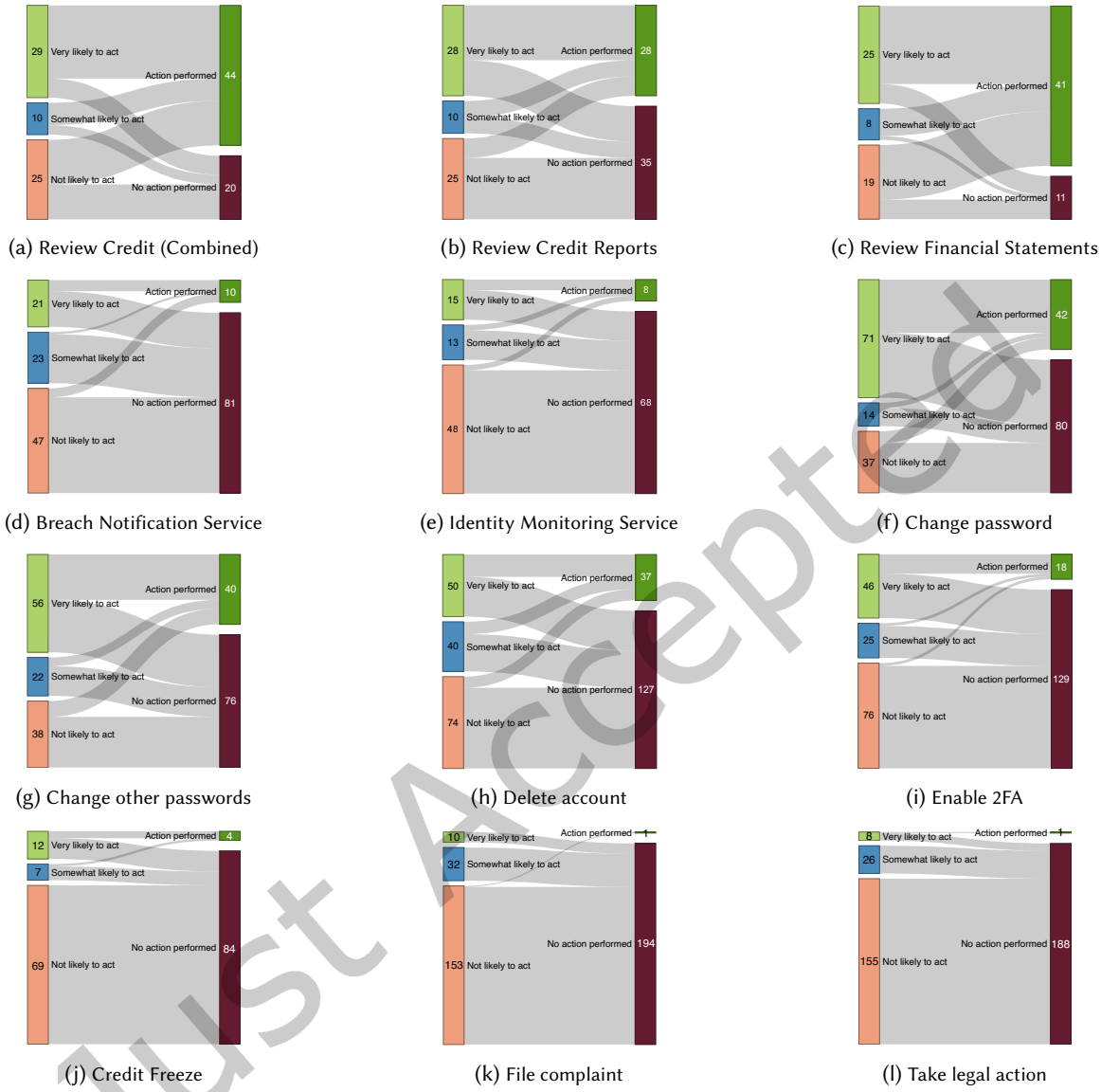
To identify which factors might predict participants' execution of any of the actions we provided, we re-ran the regression analysis from Section 4.5. This time, we added the intention as stated in the main survey as an independent variable and used participants' close-ended responses of whether they had performed any of the actions as the dependent variable. However, the model did not converge; therefore we refrain from reporting the model's output here. Instead, we found that the results strongly depended on the respective protective action.

Therefore, in the following we describe–action by action–to what extent participants followed through with their intention to act after the main survey. The findings regarding each action begin with quantitative analyses of how well intention translates to action based on descriptive statistics and regression models. For some actions, we present additional details from qualitative responses to add more insights on how the action was executed. As a reminder, we excluded from the regression analyses all responses in which the participant indicated they had performed the action before the main survey or the action did not apply to their case. The number of valid responses for the regression analyses thus varies across different actions, and we note the specific number after each action using the "*n*=" mark. In all regression analyses, the *not likely to act*-response from the main survey was set as the baseline for the IV (represented by the intercept). An overview of the follow-through rates can be found in Figure 7.

5.1.1 Actions Applying to All Breaches We first describe how participants followed through on their intention for actions that are not specific to an individual breach and therefore would only have to be performed once to provide a protective effect in reaction to multiple breaches (e.g., signing up for an identity monitoring service).

Review credit reports and/or financial statements (*n*=64). In 44 (69%) of responses, participants reported having reviewed their credit reports and/or their financial statements. While the intention to perform any of the two actions was queried together in the main survey, we separated these two actions out in the follow-up survey. When looking at them separately, the follow-through rate of reviewing financial statements (41 out of 52, 78%) was much higher than that of reviewing credit reports (28 out of 63, 44%). The regression analysis revealed no significant correlation between the intention and action for reviewing credit reports and/or financial statements.

Participants' free text responses to Q31 and Q32 shed more light on when and how participants reviewed their credit reports and/or financial statements. In 26 cases, participants described already being proactive in reviewing financial statements even prior to participating in our research, such as a result of being affected by an older breach (e.g., *"I regularly do this and was not doing it because of the notification [in this study]. I had a data breach before and actually am supposed to receive compensation for it but never did"*). However, our study also served as a trigger for some participants to review their financial statements or credit reports afterward (e.g., *" I checked my credit report within a day or so and found many discrepancies"*). In other cases, while participants already monitored their credit reports or financial statements, our study motivated them to do it more frequently (e.g., *'I now frequently monitor my credit report to suspicious activity and look at my bank statements much more frequently. This takes minimal effort on my part and will be beneficial to me"*). The monitoring could also be integrated to services that participants already used, rather than requiring them to adopt new services (e.g., *"I*



(a) Review Credit (Combined) (b) Review Credit Reports (c) Review Financial Statements

(d) Breach Notification Service (e) Identity Monitoring Service (f) Change password

(g) Change other passwords (h) Delete account (i) Enable 2FA

(j) Credit Freeze (k) File complaint (l) Take legal action

Fig. 7. Participants' follow-through rates for different actions (2FA stands for two-factor authentication).

have Credit Karma, so after seeing the breaches, I looked a little closer at my activity to make sure there was nothing that shouldn't be there").

Sign up for breach notification services (n=91). Among the 91 valid responses, only 10 (11%) reported signing up for a breach notification service. We ran a logistic regression to examine the intention-behavior gap in this scenario. Only the intercept was significant ($Est._{intercept}$=−2.38, $OR_{intercept}$=10.75, 95% $CI_{intercept}$=[−3.58, −1.47],

$p<.001$), implying that participants with no intention to act rarely ended up signing up for a breach notification service. As shown in Figure 7d, most participants who selected "somewhat likely" and "very likely" to act did not follow through this action either.

Sign up for credit and/or identity monitoring services (n=76). Similarly to the low follow-through rate regarding breach notification services, participants mentioned signing up for a credit or identity monitoring service in only 11 (8%) responses. The regression analysis on the intention-behavior gap in this scenario showed that both the intercept ($Est._{intercept}$=−3.14, $OR_{intercept}$=23.00, 95% $CI_{intercept}$=[−4.95, −1.96], $p<.001$) and being "very likely" to act ($Est._{very\ likely}$=2.12,
$OR_{very\ likely}$=8.36, 95% $CI_{very\ likely}$=[0.37, 4.19], p=.02) were significantly correlated with the final execution of this action. This means that participants tended to stick with their intentions on both ends of the likelihood-spectrum.

Only two participants mentioned signing up for a credit/identity monitoring service after our main survey in their open-ended responses. One participant signed up for a paid version of LifeLock. The other participant signed up for an unnamed identity monitoring service in addition to a breach notification service. In another seven cases, participants mentioned already having a credit monitoring service in place before our main survey, with Credit Karma being the most popular (e.g., *"Given that I am already active on Credit Karma, it's pretty easy to check [my bank statements and credit card statements]"*).

Credit Freeze (n=88). Among the 88 valid responses, only four (5%) indicated having placed a freeze on their credit reports. All participants who stated that they were not likely to perform this action in the main survey ended up not performing this action. We refrain from reporting the regression analysis result since the model had a singularity error.

5.1.2 Actions Applying to Specific Breaches. In addition to asking about the actions that need to be performed only once in response to all breaches, we investigated those that are responses to individual breaches. To that end, we walked participants through the same breaches (up to three) as in the main survey. For each breach, we asked whether they had performed a list of seven breach-specific actions. Below we present the results. Similarly, for each action we note the number of valid responses (excluding "I've done this already" and "non applicable") for the regression analyses on the intention-behavior gap.

Change the password for affected account (n=122). In 42 (34%) responses, participants indicated that they had changed the password for their account on the breached site. The regression analysis showed that participants who reported "very likely" to act in the main survey were significantly more likely to follow through the action of changing their password ($Est._{very\ likely}$=2.69, $OR_{very\ likely}$=14.79, 95% $CI_{very\ likely}$=[1.69, 129.25], p=.01). Similarly, participants who reported "not likely" to act were significantly more likely to not act ($Est._{intercept}$=−3.04, $OR_{intercept}$=0.05, 95% $CI_{intercept}$=[0.01, 0.42], $p<.001$). These results suggest that participants stuck with their initial intention on either side of the likelihood spectrum.

Change reused passwords for other accounts (n=116). In 40 (34%) responses, participants indicated they had changed the password for other accounts that used the same password as their account on the breached site. Nevertheless, a regression analysis on the intention-behavior gap in this scenario revealed no significant results, indicating that participants' intention for changing the password for other accounts did not serve as a reliable predictor for following through this action.

Delete Account (n=116). Participants in only 37 (23%) of the 116 valid responses indicated that they deleted the account for the breached site. For the regression analysis on the intention-behavior gap, only the intercept (representing "not likely to act") showed a significant p-value ($Est._{intercept}$=−9.55, $OR_{intercept}$=< 0.001, 95% $CI_{intercept}$=[< 0.001, 0.07], p=.006), indicating that participants with little intention to delete their accounts

were very likely to keep their accounts in the end. Participants' open-ended responses shed more light on the deliberation between changing the password and deleting the account, as the latter was considered a more applicable action especially for old or rarely used accounts (e.g., *"First I changed my password, but since I really don't use this account, I went back and deleted it, which also led me to start closing accounts on sites I no longer frequent"*).

Enable two-factor authentication (n=147). Among the 147 valid responses, only 18 (12%) reported enabling two-factor authentication (2FA) for the account on the breached site. The regression analysis on the intention-behavior gap for 2FA revealed a significant p-value for the intercept ($Est._{intercept}$=−23.44, $OR_{intercept}$=15g, 95% $CI_{intercept}$=[−40.91, −5.96], p=.009) and the "very likely to act" responses ($Est._{very\ likely}$=10.64, $OR_{very\ likely}$=41k, 95% $CI_{very\ likely}$=[0.02, 21.27], p=.05). However, the magnitudes of the odds ratios potentially as a result of the small sample size and skewed data distribution mean that these results should be taken cautiously. In open-ended responses, some participants mentioned enabling 2FA as an alternative for deleting their account (e.g., *"I enabled two-factor authentication on my account because that [was] what was recommended if you didn't want to close your account"*).

Take legal action (n=189). Taking legal action, as one of the most serious and burdensome reactions, was unsurprisingly the most unpopular action: only one out of the 189 valid responses reported taking legal action. The regression analysis on the intention-behavior gap showed a non-converging model.

File a Complaint (n=194). Similar to the low adoption of taking legal action, only one out of the 194 valid responses indicated filing a complaint with a consumer protection agency for the corresponding data breach. The regression analysis on the intention-behavior gap for filing a complaint revealed that only the intercept (representing "not likely to act") showed a significant p-value ($Est._{intercept}$=−5.02, $OR_{intercept}$=151.4, 95% $CI_{intercept}$=[−7.00, −3.04], p<.001), indicating that participants with little intention to file a complaint were very likely to not do so.

Warned others about the breach (n=163). Warning others (e.g., family members, friends, and colleagues) about the breach was a new action we added to the follow-up survey to probe into the social influence of security behaviors [24, 142]. Among the 163 valid responses for this action, participants in 41 (25%) responses indicated that they had warned others about the breach since the main survey, mostly (28; 68%) within one week. In five responses participants indicated that they had warned others already even before taking our main survey. In another 74 (45%) responses, participants indicated that this action did not apply to their situation.

In open-ended responses, participants further elaborated on why and how they warned others (e.g., *"I warned a few people I know who do use CafePress or similar services. My motivation was to make sure they understood this kind of breach can happen. The experience was unremarkable; just a few conversations"*). Notably, several participants explained that they did not warn others because they did not know anyone else who used the same service (e.g., *"No one I know uses Last.fm, so I did not have anyone to warn"*).

RQ6: To what extent do participants follow through on their intentions to take action six months after the main survey?
The presence of the intention-behavior gap depends on the type of action. For some actions, such as changing the password for the affected account and signing up for credit/identity monitoring services, participants tend to follow through with their intentions across all levels. For some other actions such as deleting the account, this only applies to one side of the likelihood spectrum, i.e., participants who did not intend to delete their account tended to keep their account, but those who claimed they planned to delete their account could also end up not doing it. For other actions such as credit freezes and filing a complaint, there was a clear intention-behavior gap as intention fails to serve as a reliable predictor for action.

Action Main Survey	Action Follow-up Survey	Intention Main Survey	Behavior Follow-up Survey	Significance Follow-Through
Change Reused Passwords For Other Accounts		↑: 56/116 (48.3%) →: 23/116 (19.8%) ↓: 47/116 (40.5%)	✓: 40/116 (34.5%) ×: 76/116 (65.5%)	No sig. correlations
Change The Password For The Affected Account		↑ : 71/122 (58.2%) →: 14/122 (11.5%) ↓: 37/122 (30.3%)	✓: 42/122 (34.4%) ×: 80/122 (65.6%)	Sig. correlations Not likely → No action Very likely → Action
Review Credit/Financial Report	Review Credit Reports Review Credit Statements	↑: 29/64 (45.3%) →: 10/64 (15.6%) ↓: 25/64 (39.0%)	✓: 44/64 (68.8%) ×: 20/64 (31.2%)	No sig. correlations
Delete Account		↑: 50/164 (30.5%) →: 40/164 (24.4%) ↓: 74/164 (45.1%)	✓: 37/164 (22.6%) ×: 127/164 (77.4%)	Sig. correlation Not likely → No action
Enable 2FA		↑: 46/147 (31.3%) →: 25/147 (17.0%) ↓: 76/147 (51.7%)	✓: 18/147 (12.2%) ×: 129/147 (87.8%)	Sig. correlations Not likely → No action Very likely → Action
Sign Up For Credit and/or Identity Monitoring		↑: 15/76 (19.7%) →: 13/76 (17.1%) ↓: 48/76 (63.2%)	✓: 8/76 (10.5%) ×: 68/76 (89.5%)	Sig. correlations Not likely → No action Very likely → Action
Sign Up For Breach Notifications		↑: 21/91 (23.1%) →: 23/91 (25.3%) ↓: 47/91 (51.6%)	✓: 10/91 (11.0%) ×: 81/91 (89.0%)	Sig. correlation Not likely → No action
Freeze Credit		↑: 12/88 (13.6%) →: 7/88 (8.0%) ↓: 69/88 (78.4%)	✓: 4/88 (4.5%) ×: 84/88 (95.5%)	-†
File a Complaint		↑: 10/195 (5.1%) →: 32/195 (16.4%) ↓: 153/195 (78.5%)	✓: 1/195 (0.5%) ×: 194/195 (99.5%)	Sig. correlation Not likely → No action
Take Legal Action		↑: 8/189 (4.2%) →: 26/189 (13.8%) ↓: 155/189 (82.0%)	✓: 1/189 (0.5%) ×: 194/189 (99.5%)	-†
-*	Warn Other People	-*	✓: 41/163 (0.5%) ×: 122/163 (99.5%)	-*

Table 8. Overview of the results pertaining to intentions to act and reported behaviour. Actions ordered by intention in main survey. Intention levels: ↑ = Very likely to act, → = Somewhat likely to act, ↓ = Not likely to act. Behavior levels: ✓ = Action performed, × = No action performed. * *Warn Other People* action was not inquired in main survey and has therefore no intention measurement to correlate. † Non-converging or singularity model.

5.2 RQ7: Motivators & Impediments for Behavior

In this section, we use participants' qualitative responses to explore their motivations for taking action and the hurdles that prevent them from taking specific actions.

5.2.1 Motivations for Taking Action. In total, participants provided 163 open-ended responses (63 responses for Q31, 100 responses for Q34) for the questions that asked about their motivations for taking action. Notably, participants in a significant portion of these responses described *what* actions they took but did not delve into the *why* aspect, e.g., 53 (33%) responses mentioned changing passwords, and 49 (30%) responses mentioned reviewing information such as credit reports and bank statements. For responses that did specify the motivators, we highlight several most common ones.

Concern. In 19 (12%) responses, participants mentioned concern was their primary motivator for taking action. The concern originated from the fact that the breach occurred as well as thoughts about potential consequences, such as becoming a victim of fraud or identity theft as a result of their personal information getting leaked. For example, one participant described the shock after learning about the sheer number of breaches that involved their personal information: *"I was really shocked by how many breaches involving my personal information occurred in such a short time frame.* Another participant mentioned thinking about the possibility of identity theft, regardless of whether it happens for real, could be nerve-racking: *"Even thinking about ID theft tends to make me very nervous, so I check [my financial] statements automatically when the topic comes up."* The knowledge of being affected by one breach could also prompt participants to become concerned about their situation with other

breaches and overall digital security (e.g., *"Knowing that I was a victim of a data breach, I wondered just how much of my information was exposed. It made me concerned, and I felt I needed to be proactive to make sure my finances were safe and that I would know if such things happened again"*).

Prior Incidents. Another common motivator for taking action was prior incidents, mentioned in 15 (9%) responses. Examples of prior incidents included being affected by previous data breaches, having compromised debit/credit cards and financial accounts (e.g., PayPal), and being a victim of identity theft. In one case, the participant cited unknown transactions to their bank account as a motivator for monitoring their statements closely: *" I have fallen victim to theft of funds at least twice in the not so far past, so keeping an eye on my financial records for suspicious activity is extremely important to me."* In another case, the participant took action because their debit card was previously compromised: *"I had previously had a debit card compromised [...] I began paying closer attention to my statements."* Sometimes the fraudulent charges could be a recurring issue, making the participant more vigilant (e.g., *"Several years ago after fraudulent charges showed up on my debit card, more fraudulent charges showed up on the *replacement* card within the first couple days after I activated it, and since I've never discovered how that happened, I've remained a little paranoid"*).

Proactive Attitude Toward Security. In 14 (9%) responses, participants mentioned their motivator was a proactive rather than reactive attitude to protect themselves and their personal information. These participants believed that taking preventative measures would prevent future harms from occurring (e.g., *"I wanted to prevent any harm done from the breach and any future problems"*). Some other participants shared ongoing concerns about data breaches, warranting proactive mitigation from their perspective (e.g., *"The data breach issue is always on my mind and precautions are necessary to prevent further financial or identity theft damage or other issues"*). Moreover, preventative measures such as credit freezes could be combined with reactive measures such as checking credit reports, as one participant described: *"I placed a credit freeze to make it harder for anyone to use my data to get a credit card or loan. I reviewed my credit reports to make sure no one had already tried to use my data to apply for a loan or a credit card; it looked like no one had."*

Action-Specific Motivators. Furthermore, some motivators only apply to specific actions. For example, the account being unused/not needed stood out as a prominent reason for participants who opted to delete the account, as mentioned in 25 (15%) responses. As one participant explained: *"I no longer even used the Zynga account so it was not like I needed to keep the account open."* Some participants who saw the account's value changed the password instead, either because they were concerned about the possibility of account compromises (e.g., *"Changing my password was the quickest prevention of unauthorized access to my information"*), or because they wanted to avoid the inconvenience of losing the account (e.g., *"I change my password because I use that company quite often"*). Notably, seven participants also cited ease/little effort required as a motivator for changing passwords or deleting accounts rather than taking other measures (e.g., *"That was an easy and (relatively) painless thing to do"*).

5.2.2 Impediments To Taking Action. In total, participants provided 314 open-ended responses (102 for Q32, 212 responses for Q35) for the questions that asked about their reasons for not taking action. We next highlight several most common impediments.

Apathy/Not Concerned. In contrast to concern being a crucial motivator for taking action, apathy/not being concerned was a common reason for not taking action, appearing in 79 (25%) responses. Some participants went further to explain why they were unconcerned. For instance, in 47 (15%) cases participants believed that they *would not be targeted* when criminals seek to misuse personal information leaked in the breach. Such assessment could stem from the observation that there was no critical information involved in the account on the breached site, e.g., *"I don't care about MySpace. I didn't have any critical information on that website, so if it was breached it*

doesn't matter to me that much." Another contributor to a lack of concern was the belief that *no harm will occur* as a result of the breach, e.g., because the participants felt that they had *"no significant assets accessible online"* or *"don't have a lot of money that could be scammed."* In another ten cases, participants speculated that they were unlikely to be affected because they were already taking *proactive measures* to protect their security (e.g., *"I don't care if anyone knows most of this info. Email spam goes to any number of secondary emails. No two of my passwords are the same or even alike"*).

Cost Outweighing Benefits. Participants' open-ended responses also demonstrate a deliberate cost-benefit analysis behind their decision-making, and inaction could occur as they perceived more costs associated with taking action than potential gains. In 51 (16%) responses, participants mentioned the action in question was *unnecessary*, which mostly applied to taking legal action and filing a complaint with a regulatory entity (e.g., *"Dropbox is integral to my storage/archiving strategy. Filing complaints and legal action would be ineffective in these cases and not worth the effort"*). In another 25 (8%) responses, participants cited *inconvenience* as reasons for inaction. One participant explained: *"A breach of my online data would not yield enough of a loss to justify the time and/or expense of taking these actions."* Another participant mentioned that the efforts required for action accumulate when considering the growing number of breaches: *"From what I have seen, these breaches are so frequent; the process for dealing with them [was] so lengthy and involved that I am not going to devote that amount of time and effort to something that will happen no matter what I do."*

Financial Impediments. Financial cost is a prominent factor that goes into participants' cost-benefit analyses. In 18 (6%) cases, participants shared that they did not want to pay for services that claim to protect them. One participant questioned the effectiveness of identity theft protection services: *"I don't believe the risk of identity theft is large enough to warrant paying for a service to protect against it. I also am not quite sure what a paid service could even do to stop identity theft."* Similarly, another participant commented that credit/identity monitoring services do little to stop others from misusing their personal information: *"They can only charge me money for letting me know if someone has done so and for trying to fix the problem, something I can try to do myself."* Other participants treated costs associated with these services as an unnecessary burden on their already strained financial situation (e.g., *"I cannot afford to pay for a breach notification service. It is outside the limits of my budget"*), or did not see the need for additional paid services (e.g., *"My bank is really good with dealing with any suspicious activity for free so I didn't feel that I needed to pay anyone else extra for this service"*).

Account-related Impediments. Notably, a significant hurdle for some participants to do anything about their account on the breached site (even if they wanted to) was that they did not have an account (31; 10%) or they did not even recognize the site (18; 6%). Taking account-related action indeed became an impossible task, as one participant explained: *"I don't recall having an Ulmon account so I'm not sure how I would do any of these tasks without having one."* For participants who did manage to find their accounts, they decided the courses of action based on the account's utility, such as how often they used the account and how much sensitive personal information the account held about them. In 22 (7%) cases, participants shared that they did not follow through on the recommended actions, but instead simply deleted the account since it was old or inactive (e.g., *"I deleted the account, so there was no need for a password change or two-factor authentication"*). Conversely, nine participants mentioned that they kept the account but changed the password or deleted some personal data in it (e.g., *"I didn't delete or deactivate my Dave account because I use it as a payday loan app and it's something I feel is necessary to have"*).

'I forgot.' Unsurprisingly, participants in 29 (9%) responses attributed their reason for inaction to 'I forgot.' These participants either forgot about following through the action (e.g., *"If I changed my password, I don't remember. If I didn't, it's just because I forgot or was too lazy"*), or forgot about having an account on the breached site in the first place (e.g., *"I think I forgot all about it as I only ever used Kickstarter once and wasn't thinking I'd be*

returning"). This finding is in line with past work showing that people often have slip-ups in their security and privacy practices [78, 143], and would need reminders for things like installing security updates [37, 38]. Some participants further mentioned that participating in our follow-up survey served as a reminder for them to follow through the action (e.g., *"I forgot about doing it. No good excuse! I know that I still have the same password because I've used it recently. I plan on changing it now"*).

Resignation. Similar to findings in the main survey, participants in 24 (8%) responses conveyed a resigned sentiment toward data breaches which led them to opt for inaction. For instance, one participant described feeling that they will continue to be affected by breaches no matter what action they take: *"I figure that my information can continue to be breached, and so I can't keep paying money to stop it from being breached."* Another participant shared that they felt they could do little to repair possible damages: *"The leak had already occurred and nothing I would do would change that. I did consider telling others, but felt like pretty much everyone has been a victim of some type of leak, and I really didn't know what they (or I) should do about it."*

RQ7: What factors influence participants' execution of intended actions in response to data breaches that affected them? In analyzing participants' open-ended responses, we found that the most common motivators for taking action were a proactive attitude toward protecting their security, concern, and prior incidents. Correspondingly, participants cited a lack of concern, forgetfulness, and resignation as primary impediments to action. The rationales participants gave for inaction further reflected a cost-benefit analysis as they viewed the costs of taking certain actions (e.g., in terms of time, efforts required, and financial expenses) outweigh the potential gains. Actions such as changing the password and deleting the account on the breached site became unrealistic when participants did not recognize the site or did not recall having an account in the first place.

6 Discussion

Summary of empirical and theoretical contributions. We discuss how our findings align with or differ from prior work as below. In our main survey, we examined individuals' awareness, perception, and responses to specific data breaches that had exposed their email addresses and other information. Compared to RAND's 2016 survey [1], in which 44% reported already knowing about a breach before receiving a notification, we found that participants' prior awareness was much lower in our sample (RQ4), and participants reported a lower level of overall concern than in prior work [53, 59] (RQ5). This might result from a methodological difference, as our participants reflected on specific breaches affecting them rather than on breaches in general [1, 53] or on hypothetical scenarios [59]. Another possible reason is that participants mostly saw breaches with non-sensitive records [52], which consist of the majority of the leaked data types in the HIBP database. While the potential consequences of data breaches identified by our participants (e.g., more spam and increased risks of identity theft) are similar to those in prior work [59, 142], many of our participants considered these events would have little to no impact on their lives, which might help explain the low overall intention to act among our participants.

We then followed up with eligible participants six months later, finding that for most actions, participants' intention to act translated rarely to action (see Figure 7). This finding adds to prior literature on the intention-behavior gap in other security contexts (e.g., compliance with organizational security policies [20, 56]). We further contribute novel insights into the reasons behind this gap in the context of reacting to data breaches, as our participants mentioned a lack of concern, perceived costs outweighing benefits, and impediments related to their finance or account with the breached site as major hurdles in their attempts to translate the intention into action.

Our findings also connect with established theories about behavioral change in psychology literature, most notably the Protection Motivation Theory (PMT) [105]. PMT describes that individuals respond to a threat by considering the threat itself (threat appraisal, including threat severity and threat vulnerability), as well as their ability to respond to that threat (coping appraisal, including response efficacy, self-efficacy, and response cost).

Most of the PMT components have been found to have reliable effects on individuals' behavioral intention in the information security context [76], and they are indeed well-reflected in our results. For instance, participants' qualitative responses about apathy or a lack of concern could be interpreted as low threat perception when they believed they would not be personally targeted (low threat vulnerability) or no harm would occur as a result of the breach (low threat severity).

However, we also found situations in which PMT fails to explain participants' inaction — e.g., even if the threat and coping appraisals would lead someone to form the intention to delete their account, some websites may not offer account deletion as an option, making the respective action unfeasible. Going beyond such external factors introduced by usability issues with account settings and controls, PMT also does not include awareness, whereas our main survey findings highlight that low awareness of breaches is a key barrier to taking action. To this end, our findings are more closely related to recent work on the "security and privacy acceptance framework" (SPAF) developed by Das et al. [23], in which the authors identified awareness, motivation, and ability as three major barriers to users' acceptance of expert recommendations. Descriptively, our findings validate that awareness, motivation, and ability all play an important role in individuals' adoption of self-protective behaviors after data breaches. Future work could look to quantify the relationship (e.g., via structural equation modeling) and identify factors not covered by SPAF.

Bridge the Intention-Behavior Gap. We found that the presence and magnitude of an intention-behavior gap largely depend on the specific action. Out of the ten actions we examined, only "reviewing credit reports" and "reviewing financial statements" received a >50% follow-through rate for the intention to act. While our regression results should be interpreted with caution (since we had a small sample size for the follow-up survey despite our best efforts to recruit participants back, cf. Section 3.2.2), even by looking at the descriptive statistics, it is safe to conclude that intention did not serve as a reliable predictor for action in the context of people's reactions after data breaches. Our findings align with prior work on the intention-behavior gap in other contexts [113, 134]. We encourage future security research to continue examining the intention-behavior gap and measure people's actual behavior when possible, ideally by combining self-reported and real-world measurement data to yield complementary insights [100].

Knowing this gap exists, how can we help people transform their intentions into actual behavior? Prior work has highlighted various self-regulatory challenges people may face in realizing their intentions [42, 113] (e.g., forgetting to act and experiencing disruptions) that interventions can target accordingly. Recent security research has also contributed promising examples. For example, Frik et al. showed how reminders and commitment nudges (i.e., pre-committing to a time of installation) helped their participants follow through with the intention to install security updates and enable two-factor authentication [38]. Story et al. showed how implementation nudges (i.e., helping participants form concrete and contextually activated plans) worked to increase the adoption of secure mobile payments [119]. In our study, several participants indeed mentioned that they did not follow through with their intention because they forgot, not because they did not want to or could not do so in their condition, and our follow-up survey served as a reminder for them. We imagine that similar nudges could be implemented to help these participants realize their intentions when they are already highly motivated—such as periodic reminders to change their password, or a template they can fill out to detail their plans to place a credit freeze (e.g., the next time they pay their credit card bills). On the other hand, decreasing the effort [47] for remediating actions might also encourage more people to follow through on their intentions, e.g., by providing automation tools for the remediation [75].

Consider the Effort Budget and Situations of Individuals. Our research joins related work [51, 53, 142] in painting a bleak picture of consumers' limited action after data breaches. However, our analyses of participants' open-ended responses provide rich insights into the impediments to action, suggesting a certain extent of cost-benefit analyses in participants' decision-making and that inaction should not be viewed as a purely negative outcome.

In particular, a fair number of participants in the follow-up survey mentioned account-related impediments that mostly apply to actions related to their account with the breached site, such as changing the breached password and deleting the account. Some of them did not recognize the breached site, some did not believe they had an account with the breached site (which is likely to be the case when the site is a business-to-business company or data broker), and others struggled to recover their account. Even for participants who were in a position to take account-related protective measures, some argued that the cost of taking action accumulated and it was unrealistic for them to react to every single breach.

These findings suggest that we need to develop a more nuanced view of consumers' inaction in the face of data breaches, or even in the face of security and privacy threats in general. For example, a direction for future work could be empirically tracking and measuring the impact of being affected by breaches, ideally in a longitudinal setting. Most consumers may care more about concrete forms of harm such as monetary loss, rather than psychological harm (especially if they are not experiencing anxiety or other emotional distress as a result) or the likelihood of future harm that is mostly used in courts for breach-related lawsuits [117]. For consumers who are not experiencing negative events, like identity theft, as a result of being affected by the breach, their inaction could be well justified considering their limited compliance budget [47] and competing needs in daily lives. In fact, in a recent measurement study, Breen et al. [13] report that the six cybercrimes they studied—representing almost 30% of cybercrime in the U.S.—are rare, with none having an estimated annual prevalence rate above 3.5% among the US population (scaled up from the participants in their representative sample). Considering the cost of taking action and the prevalence of cybercrime, it is a big ask for consumers to adopt every possible protective measure for every breach. Therefore, theories such as the privacy calculus [28] might be appropriate to model individuals' behavior in the response to data breaches. Their application should be considered in future studies.

Relatedly, another direction for future work could be developing and evaluating mechanisms of providing affected consumers with advice on actions personalized to their situations. For example the action "change the password for the affected account" would not make sense and should not be recommended if passwords were not among the types of breached data. Another way of further reducing consumers' burden and fatigue is to recommend the action only to users who still have an active account with the breached site based on automated detection. Similar efforts have appeared in commercial breach notification products, e.g., BreachIQ[8] claims to provide "customized action plans based on an individual's unique breach history and risk exposure — providing their own dynamic Identity Safety Score." Such personalized advice might help consumers better prioritize actions to take — an improvement compared to existing letter-based breach notifications [141]. However, more research is needed to understand whether personalized rather than one-size-fits-all advice indeed improves the security outcomes for affected consumers as well as any potential biases in the personalization algorithms.

Address misconceptions. Despite the rational aspects of inaction, participants' open-ended responses in both the main and follow-up surveys still reflect misconceptions that need to be addressed. In some cases, misconceptions become hurdles for considering, not to mention adopting, protective measures (e.g., one participant commented that they could not afford to pay for a breach notification service, whereas in reality most of these services are free). Clarifying these misconceptions in consumer-facing messages could be a way forward to encourage the adoption of protective measures.

Misconceptions also exist in participants' perceptions regarding the causes and consequences of data breaches. Specifically, most participants blamed their own email habits or security practices for data breaches, and such misconceptions exacerbate a power asymmetry — rather than demanding that organizations improve security measures or that regulators hold them accountable, participants blamed themselves. As our participants mentioned, actions like filing a lawsuit or filing a complaint with regulatory entities might indeed be perceived as time-intensive (irrespective of the actual time needed) and therefore perceived as beyond reach for an average consumer.

[8]https://www.sontiq.com/breachiq/

However, affected individuals can join forces via collective action to demand redress and fight against the power chasm between data harvesting institutions and individual users [22, 138]. Recent work has suggested a design space for online platforms to help affected consumers coordinate and connect them with expert stewards who can translate the demands into concrete requests for recourse [138]. In assessing a breach's impact, participants' responses further reflect an interesting pattern: those who had not experienced concrete adverse impacts mostly did not take the breach seriously, whereas those who had experienced an adverse event (which they believed to have resulted from the breach) reported emotional distress and resulting behavioral changes. This finding aligns with prior work on the role of present bias [68]—discounting future risks in favor of immediate gratifications—in people's security behaviors [37, 38]. Consequently, nudging interventions can seek to help consumers better visualize the concrete harms of data breaches and use high-risk situations (e.g., right after accidentally clicking on a phishing link) as valuable education opportunities to communicate advice.

When developing and implementing nudges that address misconceptions and encourage consumers' reactions, ethics are an important aspect to consider [102]. Our findings show the key role of concern in individuals' processes of forming intentions and taking action after breaches. As such, it might be tempting to focus on how we could trigger consumers to be more concerned when designing respective nudges. Yet, following this approach requires great care and caution. Prior work has shown that fear appeals alone could be mildly effective at most, especially when they are not used in combination with messages about coping strategies [127]. Recent work on trauma-informed computing [17] further suggests that many established approaches to induce fear in security warnings (e.g., using words like "danger" or "threat") could trigger panic or hypervigilance for trauma survivors, especially when considering that experiencing data breaches (and associated consequences such as identity theft) itself could be traumatic. We need more research to tackle this tension between informing consumers of risks and actions after breaches versus accounting for the possible effects of trauma on their reactions.

Develop better tools to help consumers react to breaches. While consumers may not be able to prevent breaches from happening, they can take action to mitigate the aftermath of a breach. Our findings show that some straightforward actions such as changing passwords had relatively high adoption rates and intention to adopt; participants also followed through on their intentions for these actions. Yet, the majority of actions we examined were much less popular, indicating the need to offer more usable and useful protective measures to affected individuals. Decreasing the effort required to perform these actions could directly influence the response cost, one of the factors postulated to influence behavior as part of Protection Motivation Theory, as we already discussed before.

One of our key findings is that extensive use of an email account significantly increased the email address's likelihood of being involved in a breach. Yet, simply asking users to reduce their usage or abandon their email accounts is not a viable solution, as it also diminishes the email account's utility. Instead, drawing from some participants' descriptions of creating dedicated email accounts for registration on low-value sites, we see the promise of more automated tools to offer unique email aliases for account registration. Such features could further be integrated into other technologies with broader adoption, such as browsers or password managers, to create a more streamlined experience through features like auto-filling. Recent respective efforts include "Sign in with Apple"[9] and Firefox Relay[10]: both support the generation of a unique, random email address during account registration, which is forwarded to a user's actual inbox. However, both products are currently limited to their respective ecosystems. The effectiveness, awareness, and adoption of such tools, as well as how individuals manage multiple email aliases in general, are open questions for future research.

[9]https://support.apple.com/en-us/HT210318
[10]https://blog.mozilla.org/firefox/firefox-relay/

Set stricter legal requirements for notifying and protecting consumers. Our study reflects the sad reality that many individuals are unaware that they are affected by breaches, at least for breaches exposing email addresses. Current breach notification requirements, mechanisms, and tools fail to reach data breach victims, despite awareness being a crucial trigger for taking action according to regression results of our main survey. While prior work highlights the role of media in shaping consumers' attitudes toward breaches [1, 24], our participants mostly learned about the breach from the affected business or third-party services.

Regarding when to send breach notifications, one may argue that regulators need to mandate companies to send more breach notifications in order to better raise consumers' awareness of breaches. For instance, notifications should be required for *all* breaches, rather than breaches that "result in a high risk to data subjects" as in the General Data Protection Regulation (GDPR), especially when court cases are already struggling to assess risks and harms caused by data breaches [117]. Furthermore, breached businesses could be mandated to notify consumers in multiple channels instead of the most convenient one and obtain confirmation from victims that the notification was received. That being said, we should also consider the additional burden and stress passed on to consumers from having a slew of notifications sent to them irrespective of the severity of the breach and consumers' own preferences. Future research is needed to understand to what extent stricter legal requirements about when to notify consumers of breaches impact consumers' awareness as well as fatigue, similar to recent work that measures the effect of privacy laws (e.g., GDPR and California Consumer Privacy Act) on privacy policies and opt-outs for the sale of personal information [27, 74, 87, 128].

Regarding how to send breach notifications, there are opportunities for incorporating recent research and innovations in notification mechanisms into legal requirements. Prior research on SSL/TLS warnings [4, 35, 36] shows that in-browser warnings effectively raise threat awareness and encourage safer practices. Similarly, data breach notifications could explore approaches beyond letters and emails, such as in-situ methods whereby visiting affected sites leads to a notification [26], as recently pursued by some browsers and password managers that warn users if saved passwords appeared in credential dumps [69, 93]. Notifications should also consider non-adherence, as our participants reported low follow-through rates for their intentions and expressed emotions like fatigue and resignation. Drawing from warning design literature on mitigating fatigue in email-based notifications [9, 67], one could build systems that highlight unread breach notifications in email clients, similar to Gmail's reminders to reply to emails [14]. The contents of such emails could also be automatically parsed and reformatted to guide attention to important details.

To summarize, our findings about participants' lack of awareness and self-protection indicates that breached businesses should play a more active role in protecting affected individuals. Notifications should continue to exist as they give consumers the right to know, but notifying consumers should not absolve breached businesses from further responsibility — they should further ensure that consumers have viable remediation solutions and assist in the recovery process, such as offering support in identity restoration. We need to rethink the current approach of defaulting to offering credit and identity monitoring services as compensation, which are known to provide limited preventative protection [64], and our participants reported little interest in these services due to low perceived effectiveness and associated financial cost. Instead, breached businesses could offer affected consumers email alias generators, password managers, or other more promising mitigation tools by partnering with respective service providers. Regulators should also set and frequently revisit requirements for the types of services breached businesses must offer as compensation.

Importantly, breached businesses have financial incentives for transparent post-breach communications and active mitigation. Prior work shows that data breach notifications provide a venue for impression management and repairing damaged trust [55]. Moreover, breached businesses that provide affected individuals with compensation face a lower likelihood of lawsuits [107]. Regulators should also create meaningful incentives for organizations to act accordingly. For instance, the GDPR's threat of substantial fines has resulted in a heightened effort by organizations worldwide to overhaul their privacy and security programs.

7 Conclusion

Our study provides insights into individuals' awareness, perception, and responses to data breaches. We applied a novel method that presented participants with specific data breaches exposing their email addresses and other information. Findings from our main survey reveal participants' low awareness of breaches that affected them, low concern regarding the experienced breaches, and how these two factors play an important role in participants' adoption of the ten protective measures we provided. We found misconceptions in participants' open-ended responses about their perceived causes and impacts of being involved in these breaches. Our follow-up survey identifies a sizable intention-behavior gap and provides additional insights into participants' motivations and hurdles in following through their intentions to act. We outline potential avenues for addressing these identified issues — understanding the (ir)rationality behind inaction, developing interventions that bridge the intention-behavior gap and address misconceptions, and strengthening requirements for breached organizations to better notify consumers and provide mitigation tools.

Acknowledgements

This research was partially supported by a NortonLifeLock Graduate Fellowship and the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS).

References

[1] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky. 2016. *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* Technical Report. Rand Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Wang Yang, and Shomir Wilson. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *Comput. Surveys* 50, 3 (2017), 44:1–44:41. https://doi.org/10.1145/3054926

[3] Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4, 1 (2018), tyy006–. https://doi.org/10.1093/cybsec/tyy006

[4] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 257–272. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf

[5] Abdullah M. Algarni and Yashwant K. Malaiya. 2016. A Consolidated Approach for Estimation of Data Security Breach Costs *(2016 2nd International Conference on Information Management (ICIM))*. 26–39. https://doi.org/10.1109/infoman.2016.7477530

[6] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. 2015. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies* 82 (2015), 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

[7] J. Craig Anderson. 2013. Identity theft growing, costly to victims. https://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/.

[8] Julio Angulo and Martin Ortlieb. 2015. "WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 19–38. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-angulo.pdf

[9] Eric Bachura, Rohit Valecha, Rui Chen, and Raghav H Rao. 2017. Modeling public response to data breaches. In *23rd Americas Conference on Information Systems*. Association for Information Systems, Atlanta, GA, USA, 43:1–43:10. https://core.ac.uk/download/pdf/301372705.pdf

[10] Susanne Barth and Menno DT De Jong. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038–1058.

[11] Fabio Bisogni. 2016. Proving limits of state data breach notification laws: Is a federal law the most adequate solution? *Journal of Information Policy* 6, 1 (2016), 154–205. https://doi.org/10.5325/jinfopoli.6.2016.0154

[12] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2010. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2010), 18–26. https://doi.org/10.1109/MSP.2010.198

[13] Casey Breen, Cormac Herley, and Elissa M Redmiles. 2022. A Large-Scale Measurement of Cybercrime Against Individuals. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 122:1–122:41. https://doi.org/10.1145/3491102.3517613

[14] Scott Brown. 2018. Did you forget to reply to an email? The new Gmail will remind you. https://www.androidauthority.com/gmail-nudges-feature-865435/.
[15] Mohamad Adam Bujang, Nadiah Sa'at, Tg Mohd Ikhwan Tg Abu Bakar, et al. 2018. Sample size guidelines for logistic regression from observational studies with large population: emphasis on the accuracy between statistics and parameters based on real life clinical data. *Malays. J. Med Sci.* 25, 4 (2018), 122. https://doi.org/10.21315/mjms2018.25.4.12
[16] Hsiangting Shatina Chen and Tun-Min Jai. 2019. Trust fall: data breach perceptions from loyalty and non-loyalty customers. *The Service Industries Journal* 41, 13-14 (2019), 947–963. https://doi.org/10.1080/02642069.2019.1603296
[17] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 544:1–544:20. https://doi.org/10.1145/3491102.3517475
[18] Ben C.F. Choi, Sung S. Kim, and Zhenhui (Jack) Jiang. 2016. Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems* 33, 3 (2016), 904—933. https://doi.org/10.1080/07421222.2015.1138375
[19] CNBC. 2013. Target gives 10% discount to shoppers after data breach. https://www.cnbc.com/2013/12/20/target-gives-10-discount-to-shoppers-after-data-breach.html.
[20] Robert E Crossler, James H Long, Tina M Loraas, and Brad S Trinkle. 2014. Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems* 28, 1 (2014), 209–226. https://doi.org/10.2308/isys-50704
[21] Sauvik Das, Laura A Dabbish, and Jason I Hong. 2019. A typology of perceived triggers for end-user security and privacy behaviors. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 97–115. https://www.usenix.org/system/files/soups2019-das.pdf
[22] Sauvik Das, W Keith Edwards, DeBrae Kennedy-Mayo, Peter Swire, and Yuxi Wu. 2021. Privacy for the People? Exploring Collective Action as a Mechanism to Shift Power to Consumers in End-User Privacy. *IEEE Security & Privacy* 19, 5 (2021), 66–70. https://doi.org/10.1109/MSEC.2021.3093135
[23] Sauvik Das, Cori Faklaris, Jason I. Hong, and Laura A. Dabbish. 2022. The Security and Privacy Acceptance Framework. *Foundations and Trends in Privacy and Security* 5, 1-2 (2022), 1–143. https://doi.org/10.1561/3300000026
[24] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1:1–1:12. https://doi.org/10.1145/3173574.3173575
[25] Behnam Dayanim and Edward George. 2018. Data breach litigation and regulatory enforcement: A survey of our present and how to prepare for the future. *Cyber Security* 1, 4 (2018), 301–315. https://www.ingentaconnect.com/content/hsp/jcs/2018/00000001/00000004/art00003
[26] Joe DeBlasio, Stefan Savage, Geoffrey M Voelker, and Alex C Snoeren. 2017. Tripwire: Inferring internet site compromise. In *Proceedings of the Internet Measurement Conference*. ACM, New York, NY, USA, 341–354. https://doi.org/10.1145/3131365.3131391
[27] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. In *Network and Distributed Sys. Security Symp.* Internet Society.
[28] Tobias Dienlin and Miriam J. Metzger. 2016. An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication* 21, 5 (08 2016), 368–383. https://doi.org/10.1111/jcc4.12163 arXiv:https://academic.oup.com/jcmc/article-pdf/21/5/368/19946859/jjcmcom0368.pdf
[29] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* 45, 3 (2015), 285–297. https://doi.org/10.1002/ejsp.2049
[30] Digital Shadows Photon Research Team. 2019. *From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover*. Technical Report. Digital Shadows. https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover
[31] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. 2014. On the (in) security of mobile two-factor authentication. In *International Conference on Financial Cryptography and Data Security*. Springer, London, UK, 365–383. https://doi.org/10.1007/978-3-662-45472-5_24
[32] Nora A Draper and Joseph Turow. 2019. The corporate cultivation of digital resignation. *New Media & Society* 21, 8 (2019), 1824–1839. https://doi.org/10.1177/1461444819833331
[33] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 1065–1074. https://doi.org/10.1145/1357054.1357219
[34] European Parliament. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[35] Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL warnings: Comprehension and adherence. In *Proceedings of the Conference on Human Factors in Computing*

Systems (CHI). ACM, New York, NY, USA, 2893–2902. https://doi.org/10.1145/2702123.2702442

[36] Adrienne Porter Felt, Robert W Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 2667–2670. https://doi.org/10.1145/2556288.2557292

[37] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. 2016. Do or do not, there is no try: user engagement may not improve security outcomes. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 97–111. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-forget.pdf

[38] Alisa Frik, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. 2019. A promise is a promise: the effect of commitment devices on computer security intentions. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 604:1–604:12. https://doi.org/10.1145/3290605.3300834

[39] Kevin P. Gallagher, Xiaoni Zhang, and Vickie Coleman Gallagher. 2016. Measuring The Organizational Impact of Security Breaches: Patterns of Factors and Correlates. In *CONF-IRM 2016 Proceedings (Information Management & Computer Security, Vol. 11)*. 74–83. https://doi.org/10.1108/09685220310468646

[40] Gemalto. 2018. *Data Breaches & Customer Loyalty 2017*. Technical Report. Thales. https://www6.thalesgroup.com/2017-data-breaches-customer-loyalty-report

[41] Peter M Gollwitzer. 1999. Implementation intentions: strong effects of simple plans. *American Psychologist* 54, 7 (1999), 493–503.

[42] Peter M Gollwitzer and Paschal Sheeran. 2006. Implementation intentions and goal achievement: A meta-analysis of effects and processes. *Advances in Experimental Social Psychology* 38 (2006), 69–119. https://doi.org/10.1016/S0065-2601(06)38002-1

[43] Google. 2014. Cleaning up after password dumps. https://security.googleblog.com/2014/09/cleaning-up-after-password-dumps.html.

[44] Claire Greene and Joanna Stavins. 2017. Did the Target data breach change consumer assessments of payment card security? *Journal of Payments Strategy & Systems* 11, 2 (2017), 121–133. https://www.ingentaconnect.com/content/hsp/jpss/2017/00000011/00000002/art00004

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

[46] Zahra Hassanzadeh, Sky Marsen, and Robert Biddle. 2020. We're Here to Help: Company Image Repair and User Perception of Data Breaches. In *Graphics Interface Conference*. CHCCS/SCDHM, Toronto, Canada, 1–10. https://openreview.net/pdf?id=790fK3eKe4

[47] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the New Security Paradigms Workshop*. ACM, New York, NY, USA, 133–144. https://doi.org/10.1145/1719030.1719050

[48] Anat Hovav and Paul Gray. 2014. The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems* 34, 50 (2014), 893—912. https://doi.org/10.17705/1cais.03450

[49] Troy Hunt. 2020. Have I Been Pwned: Check if you have an account that has been compromised in a data breach. https://haveibeenpwned.com/.

[50] Identity Theft Resource Center. 2021. *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends, and Workplaces*. Technical Report. Identity Theft Resource Center. https://www.idtheftcenter.org/event/2021-consumer-aftermath-report/

[51] Identity Theft Resource Center. 2022. *2021 Annual Data Breach Report*. Technical Report. https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[52] Identity Theft Resource Center. 2022. Nonsensitive Records Count. https://www.idtheftcenter.org/glossary/nonsensitive-records-count/.

[53] Ponemon Institute. 2014. *The Aftermath of a Data Breach: Consumer Sentiment*. Technical Report. Ponemon Institute. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

[54] Markus Jakobsson. 2018. Two-factor inauthentication–the rise in SMS phishing attacks. *Computer Fraud & Security* 2018, 6 (2018), 6–8. https://doi.org/10.1016/S1361-3723(18)30052-6

[55] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 2014. 'All that glitters is not gold': The role of impression management in data breach notification. *Western Journal of Communication* 78, 3 (2014), 337–357. https://doi.org/10.1080/10570314.2013.866686

[56] Jeffrey Jenkins, Alexandra Durcikova, and Jay F Nunamaker Jr. 2021. 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 (2021), 1. https://aisel.aisnet.org/jais/vol22/iss1/1/

[57] Rhoda C Joseph. 2017. Data breaches: Public sector perspectives. *IT Professional* 20, 4 (2017), 57–64. https://doi.org/10.1109/MITP.2017.265105441

[58] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 39–52. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf

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

[60] Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer. 2013. A Comparison of American and German Folk Models of Home Computer Security. Human Aspects of Information Security, Privacy, and Trust, Vol. 8030. 100 – 109. https://doi.org/10.1007/978-3-642-39345-7_11

[61] Mark J Keith, Samuel C Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies* 71, 12 (2013), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

[62] Murat Kezer, Barış Sevi, Zeynep Cemalcilar, and Lemi Baruh. 2016. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1 (2016), 2:1–2:20. https://doi.org/10.5817/CP2016-1-2

[63] Bokyung Kim, Kristine Johnson, and Sun-Young Park. 2017. Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management* 4, 1 (2017), 1–17. https://doi.org/10.1080/23311975.2017.1354525

[64] Brian Krebs. 2014. Are Credit Monitoring Services Worth It? https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/.

[65] Thomas Kude, Hartmut Hoehle, and Tracy Ann Sykes. 2017. Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *Intl. J. of Operations & Production Mgmt.* 37, 1 (2017), 56–74. https://doi.org/10.1108/IJOPM-03-2015-0156

[66] Oksana Kulyk, Benjamin Reinheimer, Lukas Aldag, Nina Gerber, Peter Mayer, and Melanie Volkamer. 2020. Security and Privacy Awareness in Smart Environments – A Cross-Country Investigation *(Asia USEC)*.

[67] Juhee Kwon and M Eric Johnson. 2015. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?. In *Workshop on the Economics of Information Security*. WEIS, Amsterdam, Netherlands, 1–33. https://econinfosec.org/archive/weis2015/papers/WEIS_2015_kwon.pdf

[68] David Laibson. 1997. Golden eggs and hyperbolic discounting. *The Quarterly Journal of Economics* 112, 2 (1997), 443–478. https://doi.org/10.1162/003355397555253

[69] Ravie Lakshmanan. 2019. Chrome and Firefox will now alert you about data breaches involving your accounts. https://thenextweb.com/security/2019/10/23/chrome-and-firefox-will-now-alert-you-about-data-breaches-involving-your-accounts/.

[70] J Richard Landis and Gary G Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* 33, 1 (1977), 159–174. https://doi.org/10.2307/2529310

[71] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How effective is anti-phishing training for children?. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 229–239. https://www.usenix.org/system/files/conference/soups2017/soups2017-lastdrager.pdf

[72] Benedikt Lebek, Jörg Uffen, Michael H Breitner, Markus Neumann, and Bernd Hohler. 2013. Employees' information security awareness and behavior: A literature review. In *Hawaii International Conference on System Sciences*. IEEE, 2978–2987. https://doi.org/10.1109/HICSS.2013.192

[73] Ron Lieber. 2019. How to Protect Yourself After the Equifax Breach. https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

[74] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 47–64.

[75] Peter Mayer, Hermann Berket, and Melanie Volkamer. 2016. Enabling Automatic Password Change in Password Managers Through Crowdsourcing *(International Conference on Passwords)*.

[76] Peter Mayer, Alexandra Kunz, and Melanie Volkamer. 2017. Reliable Behavioural Factors in the Information Security Context. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (Reggio Calabria, Italy) *(ARES '17)*. Association for Computing Machinery, New York, NY, USA, Article 9, 10 pages. https://doi.org/10.1145/3098954.3098986

[77] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *USENIX Security Symposium*. USENIX Association, 393–410. https://www.usenix.org/conference/usenixsecurity21/presentation/mayer

[78] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. 2021. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 375–392. https://www.usenix.org/system/files/sec21-mcdonald.pdf

[79] Rebecca T Mercuri. 2003. Analyzing security costs. *Commun. ACM* 46, 6 (2003), 15–18. https://doi.org/10.1145/777313.777327

[80] Vyacheslav Mikhed and Michael Vogan. 2015. Out of sight, out of mind: consumer reaction to news on data breaches and identity theft. https://ssrn.com/abstract=2691902

[81] Vyacheslav Mikhed and Michael Vogan. 2018. How data breaches affect consumer credit. *Journal of Banking & Finance* 88 (2018), 192–207. https://doi.org/10.1016/j.jbankfin.2017.12.002

[82] Saif M. Mohammad and Peter D. Turney. 2013. Crowdsourcing a Word-Emotion Association Lexicon. *Computational Intelligence* 29, 3 (2013), 436–465. https://doi.org/10.1111/j.1467-8640.2012.00460.x
[83] Mozilla. 2022. Firefox Monitor. https://monitor.firefox.com/.
[84] Steven Muzatko and Gaurav Bansal. 2018. Timing of data breach announcement and e-commerce trust. In *Proceedings of Midwest Association for Information Systems Conference*. Association for Information Systems, Atlanta, GA, USA, 7:1–7:8. https://core.ac.uk/download/pdf/301374905.pdf
[85] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. of Consumer Affairs* 41, 1 (2007), 100–126.
[86] Donald A Norman. 1983. Some observations on mental models. In *Mental models*, Dedre Gentner and Albert L Stevens (Eds.). Hillsdale, New York, NY, USA, Chapter 1, 7–14. https://doi.org/10.4324/9781315802725-5
[87] Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. (Un) clear and (In) conspicuous: The right to opt-out of sale under CCPA. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. 59–72.
[88] Stefan Palan and Christian Schitter. 2018. Prolific.ac – A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27. https://doi.org/10.1016/j.jbef.2017.12.004
[89] Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 295–310. https://doi.org/10.1145/3133956.3133973
[90] Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, and Gang Wang. 2019. What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proceedings of the Asia Conference on Computer and Communications Security*. ACM, New York, NY, USA, 181–192. https://doi.org/10.1145/3321705.3329818
[91] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 518:1–518:15. https://doi.org/10.1145/3290605.3300748
[92] Rachael M Peters. 2014. So you've been notified, now what: The problem with current data-breach notification laws. *Arizona Law Review* 56 (2014), 1171–1202.
[93] Katie Petrillo. 2018. Protect Your Accounts with Breach Alerts Through LastPass. https://blog.lastpass.com/2018/11/protect-your-accounts-with-breach-alerts-through-lastpass/.
[94] Privacy Rights Clearinghouse. 2020. Data Breaches. https://privacyrights.org/data-breaches.
[95] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. 2020. "I Have a Narrow Thought Process": Constraints on Explanations Connecting Inferences and Self-Perceptions. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 457–488. https://www.usenix.org/system/files/soups2020-rader.pdf
[96] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144. https://doi.org/10.1093/cybsec/tyv008
[97] Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. *Anonymity, Privacy, and Security online*. Technical Report. Pew Research Center. https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf
[98] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *IEEE Symposium on Security and Privacy*. IEEE, Piscataway, NJ, USA, 272–288. https://doi.org/10.1109/SP.2016.24
[99] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *USENIX Security Symposium*. USENIX Association, Berkeley, CA, USA, 89–108. https://www.usenix.org/system/files/sec20-redmiles.pdf
[100] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. 2018. Asking for a friend: Evaluating response biases in security user studies. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 1238–1255. https://doi.org/10.1145/3243734.3243740
[101] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 simple steps to stay safe online: security advice for non-tech-savvy users. *IEEE Security & Privacy* 15, 5 (2017), 55–64. https://doi.org/10.1109/MSP.2017.3681050
[102] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35. https://doi.org/10.1016/j.ijhcs.2018.05.011
[103] William Roberds and Stacey L Schreft. 2009. Data breaches and identity theft. *Journal of Monetary Economics* 56, 7 (2009), 918–929. https://doi.org/10.1016/j.jmoneco.2009.09.003
[104] Steve Roberts. 2018. Learning lessons from data breaches. *Network Security* 2018, 11 (2018), 8–11. https://doi.org/10.1016/S1353-4858(18)30111-9
[105] R W Rogers. 1975. A protection motivation theory of fear appeals and attitude change. *The journal of psychology* (1975).

[106] Sasha Romanosky. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* 2, 2 (2016), 121–135. https://doi.org/10.1093/cybsec/tyw001
[107] Sasha Romanosky, David Hoffman, and Alessandro Acquisti. 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies* 11, 1 (2014), 74–104. https://doi.org/10.1111/jels.12035
[108] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management* 30, 2 (2011), 256–286. https://doi.org/10.1002/pam.20567
[109] Johnny Saldaña. 2015. *The Coding Manual for Qualitative Researchers.* Sage Publications, Thousand Oaks, CA, USA.
[110] Frederic Schlackl, Nico Link, and Hartmut Hoehle. 2022-06. Antecedents and consequences of data breaches: A systematic review. *Information & Management* 59, 4 (2022-06), 103638. https://doi.org/10.1016/j.im.2022.103638
[111] Robert Schoshinski. 2019. Equifax data breach: Pick free credit monitoring. https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring.
[112] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. 2014. "My religious aunt asked why I was trying to sell her viagra": experiences with account hijacking. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 2657–2666. https://doi.org/10.1145/2556288.2557330
[113] Paschal Sheeran and Thomas L Webb. 2016. The intention–behavior gap. *Social and Personality Psychology Compass* 10, 9 (2016), 503–518. https://doi.org/10.1111/spc3.12265
[114] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 373–382.
[115] Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 2347–2356. https://doi.org/10.1145/2556288.2557421
[116] Paul Slovic, Melissa L Finucane, Ellen Peters, and Donald G MacGregor. 2004. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis* 24, 2 (2004), 311–322. https://doi.org/10.1111/j.0272-4332.2004.00433.x
[117] Daniel J Solove and Danielle Keats Citron. 2017. Risk and anxiety: A theory of data-breach harms. *Texas Law Review* 96 (2017), 737–786.
[118] Daniel J Solove and Woodrow Hartzog. 2022. *Breached!: Why Data Security Law Fails and How to Improve it.* Oxford University Press.
[119] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From intent to action: Nudging users towards secure mobile payments. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 379–415. https://www.usenix.org/system/files/soups2020-story.pdf
[120] Qizhang Sun, Martijn C Willemsen, and Bart P Knijnenburg. 2020. Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Computers & Security* 97 (2020), 101924.
[121] Rahul Telang. 2015. Policy framework for data breaches. *IEEE Security & Privacy* 13, 1 (2015), 77–79. https://doi.org/10.1109/MSP.2015.12
[122] The Federal Trade Commission. 2019. Credit Freeze FAQs. https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.
[123] The Federal Trade Commission. 2020. When Information Is Lost or Exposed. https://www.identitytheft.gov/databreach.
[124] The Firefox Frontier. 2019. What to do after a data breach. https://blog.mozilla.org/firefox/what-to-do-after-a-data-breach/.
[125] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. 2017. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 1421–1434. https://doi.org/10.1145/3133956.3134067
[126] Dana Turjeman and Fred M Feinberg. 2019. When the Data Are Out: Measuring Behavioral Changes Following a Data Breach. https://doi.org/10.2139/ssrn.3427254
[127] René van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003
[128] Maggie Van Nortwick and Christo Wilson. 2022. Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA? *Proc. Priv. Enhancing Technol.* 2022, 1 (2022), 608–628.
[129] Jennifer R Veltsos. 2012. An analysis of data breach notifications as negative news. *Business Communication Quarterly* 75, 2 (2012), 192–207. https://doi.org/10.1177/1080569912443081
[130] Paul Wagenseil. 2019. What to Do After a Data Breach. https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html.
[131] Rick Wash. 2010. Folk models of home computer security. In *Symposium on Usable Privacy and Security*. ACM, New York, NY, USA, 11:1–11:16. https://doi.org/10.1145/1837110.1837125
[132] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 175–188. https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-wash.pdf
[133] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the Conference on Human Factors in Computing Systems*

(CHI). ACM, New York, NY, USA. Art. 478.
[134] Thomas L Webb and Paschal Sheeran. 2006. Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin* 132, 2 (2006), 249–268. https://doi.org/10.1037/0033-2909.132.2.249
[135] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L Mazurek, and Blase Ur. 2019. Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 149–166. https://doi.org/10.1145/3319535.3363200
[136] Kimberly A Whitler and Paul W Farris. 2017. The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research* 57, 1 (2017), 3–9. https://doi.org/10.2501/JAR-2017-005
[137] Victoria Woollaston. 2016. Facebook and Netflix reset passwords after data breaches. https://www.wired.co.uk/article/facebook-netflix-password-reset.
[138] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. "A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 32:1–32:17. https://doi.org/10.1145/3491102.3517467
[139] Achim Zeileis, Christian Kleiber, and Simon Jackman. 2008. Regression models for count data in R. *Journal of Statistical Software* 27, 8 (2008), 1–25. https://doi.org/10.18637/jss.v027.i08
[140] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, Smart Home' – Exploring End Users' Mental Models of Smart Homes. In *Mensch und Computer 2018 - Workshopband*. Gesellschaft für Informatik eV, Dresden, Germany, 408–417. https://doi.org/10.18420/muc2018-ws08-0539
[141] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 194:1–194:14. https://doi.org/10.1145/3290605.3300424
[142] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've got nothing to lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, USA, 197–216. https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf
[143] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*. ACM, New York, NY, USA, 443:1–443:15. https://doi.org/10.1145/3313831.3376570

Appendix

A Main Survey Material

A.1 Informed consent

Study Title: Awareness, Risk Perception, and Reaction Toward Data Breaches
Principal Investigators: Florian Schaub, Assistant Professor, University of Michigan
Adam Aviv, Associate Professor, George Washington University
Purpose of this Study: We are conducting a research study to understand how users 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 an online survey where you will be asked to review data breach records associated with one of your email addresses based on a public database of security breaches (haveibeenpwned.com) and answer a few questions about the displayed records. We anticipate the survey will take about 15 minutes.
Requirements: To participate in the study, you must (1) be 18 years old or older; and (2) currently live in the United States.
Benefits: You may not receive a direct benefit from participating, but this study will help us develop better systems and technologies that empower Internet users to protect themselves against data breaches.
Risks: The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during use of the Internet.
Compensation: You will be compensated $2.50 upon completing the survey.

Confidentiality: By participating in the study, you understand and agree that the University of Michigan and George Washington University 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 and consent form will be kept separate. Your research data will be stored securely and will only be accessible to the study team. By participating, you understand and agree that the data and information gathered during this study may be published in an academic journal or conference paper. You will not be asked to provide any direct personal identifiers in the study apart from your email address. *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 only in temporary storage to facilitate the lookup of data breaches your email address was involved in and will be deleted following the completion of this task. The researchers will never see your email address.*

Right to Ask Questions & Contact Information: If you have questions about this research, you may contact the study team at data-breach-hibp@umich.edu

The University of Michigan Health Sciences and Behavioral Sciences 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. Please be sure that we have answered any questions you may have about the study, and you understand what you are being asked to do. You may contact the researchers at any time by emailing data-breach-hibp@umich.edu if you think of a question later.

STATEMENT BY PERSON AGREEING TO PARTICIPATE IN THIS STUDY I have read this informed consent document and the material contained in it has been explained to me. I understand each part of the document, all my questions have been answered, and I freely and voluntarily choose to participate in this study. I can choose to withdraw from this research project at any time without penalty.

A.2 Email address-related questions

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 been disclosed in any data breaches (also called "security breaches"), using the public lookup service for data breaches haveibeenpwned.com. If your email address was involved in any data breaches, we will ask you some questions about those 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 only in temporary storage to facilitate the lookup of data breaches your email address was involved in and will be deleted following the completion of this task. The researchers will never see your email address.

To access information about breaches, your email address will be communicated to haveibeenpwned.com, a public service not operated by us, which maintains a database of data breaches involving email addresses. Communication with haveibeenpwned.com will occur on secure and encrypted channels, and haveibeenpwned.com also does not permanently store email addresses used in queries. As described in their privacy policy: "Searching for an email address only ever retrieves the address from storage then returns it in the response, the searched address is never explicitly stored anywhere."

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]

(2) Thank you for providing your email address. Please tell us more about this email address. 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
(4) What do you use this email account for? Choose all that apply. ○ For professional correspondence (e.g., with colleagues, business partners) ○ For personal correspondence (e.g., friends and family members) ○ Account creation / signup for sensitive accounts (e.g., banking, taxes, etc.) ○ Account creation / signup of medium sensitive accounts (e.g., social media, online shopping) ○ Account creation / signup for low value accounts (I used it when I'm prompted to sign up but don't really care) ○ Other [free-text]
(5) Approximately for 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]

A.3 Breach-related questions

(if email not involved in a data breach) **Your email address has not been part of any of the data breaches recorded by haveibeenpwned.com.** That is great news for you, but we still would like to ask you some further questions.

(7) In your opinion, what might be reasons that your email address has not been part of any data breach? [free text]
(8) Do you believe another email address that you regularly use is more likely to have breaches? [yes/no]
(9) Would you like to take this survey with that email address instead? [yes/no] *(if yes return participant to questions in Appendix A.2, if no continue to demographic questions in Appendix A.4)*

(if email involved in a data breach) **Your email address was part of a data breach:** According to haveibeenpwned.com your email address was part of one or more data breaches.

(10) In your opinion, what might be reasons that your email address has been part of data breaches? [free text]

We will now ask you questions about three of these breaches. We will show you the full data breach history for your email address at the end of the survey.

(for up to three data breach, the following …)
Your email address was part of the following breach

[img and description of breach (see Figure 1)]

Please make sure you read the description of this breach, since we will now ask you a few questions with respect to this breach (the description of the breach will be available to you while answering the questions).

(11) In your opinion, what might be reasons that your email address has been part of data breaches? [free text]
(12) Prior to this study, were you aware that you are affected by this breach? ○ yes ○ no ○ unsure
(13) *(if yes aware)* How did you first become aware that you are affected by this breach? ○ I was notified by the breached company. ○ I was notified by my bank or credit card company. ○ I was notified by a third-party breach notification service (e.g., Have I Been Pwned, Firefox Monitor, Breach Clarity). ○ I was notified by my credit monitoring or identity theft monitoring service (e.g., LifeLock, Credit Karma). ○ Someone else (e.g., a romantic partner or a family member) told me about it. ○ I found out myself through negative events in real life (e.g., suspicious activity on my credit card, locked out of online accounts.) ○ I learned about the breach through news media. ○ I do not remember. ○ Other [free text]

(14) *(if yes aware)* Please describe how you felt when you learned that your information was part of this breach *(if no/unsure aware)* Please describe how you feel after now learning that your information was part of this breach. [free text]
(15) *(if yes aware)* How concerned were you when you learned that your information was part of this breach? *(if no/unsure aware)* How concerned are you after now learning that your information was part of this breach? ○ Not at all concerned ○ Slightly concerned ○ Somewhat concerned ○ Very concerned ○ Extremely concerned
(16) *(if yes aware)* Please describe how you think this breach has or will impact your life. If you suspect or have experienced impacts resulting from this breach, please describe them.
(if no/unsure aware) Please describe how you think this breach will impact your life. If you suspect or have experienced impacts resulting from this breach, please describe them as well. [free text]
(17) How concerned are you about the following data being compromised in this breach? [for each data type in the breach as provided by HIBP] ○ Not at all concerned ○ Slightly concerned ○ Somewhat concerned ○ Very concerned ○ Extremely concerned ○ I don't know ○ Does not apply to me (the company does not have my real information)
(18) What did you do, if anything, after learning that your information was part of this breach? Please explain why. [free text]
(19) Regarding this specific breach, please select how likely you are to initiate each of the following actions within the next 30 days, or whether you have taken the action already. ○ Not likely ○ Somewhat likely ○ Very likely ○ I did/do this already ○ This does not apply to me / I don't understand
(For each of the following actions:) • Change the password of my account for the breached company, if it exists • Change the password of other accounts that used the same password • Delete or deactivate my account for the breached company, if it exists • Enable two-factor authentication on my account for the breached company, if it is available • Use a credit or identity monitoring service (e.g., LifeLock, Identity Guard, IdentityForce, Credit Karma, Credit Sesame) • Use a breach notification service (e.g., Firefox Monitor, Breach Clarity, Have I Been Pwned) • Take legal action against the breached company • Review my credit reports and/or bank/credit card statements for suspicious activity • File a complaint against the breached company with a consumer protection agency (e.g., FTC, CFPB, State Attorney General) • Place a credit freeze on my credit reports
(20) Are there any other actions you would like to initiate within the next 30 days or other actions you have already taken? [free text]

A.4 Demographics & attention checks

(21) Which of the following breaches were you asked about in this study? [multiple choice of the correct answer and four decoys]
(22) What is your age? ○ 18-24 ○ 25-29 ○ 30-34 ○ 35-39 ○ 40-44 ○ 45-49 ○ 50-54 ○ 54-59 ○ 60-64 ○ 65+ ○ Prefer not to say
(23) What is your gender? ○ Man ○ Woman ○ Non-Binary ○ Prefer not to answer ○ Other [free text]
(24) 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
(25) What is the shape of a red ball? ○ Red ○ Blue ○ Square ○ Round ○ Prefer not to answer
(26) Which of the following best describes your educational background or job field? ○ I have an education in, or work in, the field of computer science, computer engineering, or IT. ○ I do not have an education in, or work in, the field of computer science, computer engineering, or IT. ○ Prefer not to answer

(27) Which of the following best describes your educational background or job field? ○ I have an education in or work-in/practice law or other legal services. ○ I do not have an education in or work-in/practice law or other legal services. ○ Prefer not to answer
(28) 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

A.5 Debrief

Information on breaches your email address was part of: Thank you for completing our study. Please note that the information about data breaches we showed to you is real. Your email address, and potentially other personal information has been part of these breaches and could be used by criminals to steal your identity or access your accounts.

List of breaches your email address was part of: Below is the full list of breaches in which the email address you entered was involved according to haveibeenpwned.com. Please note that you can always obtain the same results by checking your email address on haveibeenpwned.com, which, in addition, also 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.

Resources for breach recovery and further reading Here is a list of resources to help you prevent or recover from harm due your information being exposed in data breaches, as well as help you better protect yourself from data breaches in the future.

- *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

B Main Survey Qualitative Codebook

In the following we provide our unified codebook with the primary codes, their respective counts, and their first-level sub-codes.

• **bad actors (17)**: *company sell data, hackers, department stores* • **behavior (94)**: *continue use as before, insecure, keep using email, secure practice, email practice, insecure practice* • **cannot recall (17)**: *confused, unconcerned, surprised, concerned* • **consequence experienced (97)**: *compromised accounts, information disclosure, spam, data on the dark web, scam, attempted login, other account with same pwd, email disclosure, identity theft, social media account hacked, physical, financial disadvantage, unrecognized new account, past event, reputation, job offer missed, upset, site breached* • **consequence potentially (92)**: *spam, identity theft, compromised accounts, information misuse, financial disadvantage, scam, physical, financial account hacked, information disclosure, stalking, other account with same password, unrecognized new account* • **data not relevant (84)**: *outdated, fake data, not sensitive, unique password, not primary email, little data, will be caught by spam filter, so much data out there, account not used, unimportant password, unique username* • **data relevant (3)**: *sensitive* • **defense intended to be put into place as reaction to breach (180)**: *change password, monitor email, use secure passwords, monitor suspicious activity, monitor financial information, do not use facebook login for shopping sites, increase protective measures,*

change email, be more cautious, 2FA enabled, limit online disclosure, review accounts, stop using, reduced use email, check suspicious emails, signing up to websites less often, new email account, learn more about breach, reduced use site, close account, scan computer frequently, re-link security accounts, change financial information, change employer, monitor accounts, use vpn, review financial information, unique password, change username, use password manager, go after companies, learn about safeguarding, solve issues as they appear, security checkup, check financial information, protective measures, stop using email, protect email, stop using service, tor, investigate, strong password, location setting, no reuse password, be more careful, legal action • **defense put into place as reaction to breach (226)**: *use password manager, change password, reduced use site, change emails, protective measures, 2FA enabled, change password creation strategy, unique password, no cc info in unused apps, actions caused by other breach, close account, change username, remove email from accounts, use secure passwords, review financial information, use breach monitors, be more cautious, review account information, update browser, check suspicious emails, change email, stop using site, nothing, changed info, check account, 2fa enabled, limit data disclosure, unsubscribed from mailer, change info, reviewed prior steps, monitoring, check financial, email practices, contacted company, changed email, unsubscribed, changed password, delete account, learn about breach, antivirus, called credit card company, recover hacked account, careful disclosure, no reuse password, strong password* • **defense put into place pro-actively before breach (40)**: *use secure passwords, 2FA enabled, be cautious, change password, don't answer phone calls, review financial information, unique password, use password manager, monitor accounts, monitor emails, unique email, protective measures, monitor credit reports, spam filter, stop using site, change email, account not used, monitor financial information* • **do not know hibpwnd (2)** • **feeling (929)**: *unconcerned, concerned, violated, annoyed, negative, skeptical, uncomfortable, fatigued, paranoid, cautious, hopeful, upset, scared, unsurprised, would have been contacted, overwhelmed, disappointed, unsure, reassured, don't care, curious, not worried, relief, insecure, no fear, worried, unhappy, not important enough, confused, indifferent, surprised, unsafe, ashamed, regret, informed, used to breaches, no blame on company, upset* • **first breach (1)** • **immediately informed (1)** • **impact (525)** *impact little, impact none, impact large, impact positive, impact unsure, impact negative, unconcerned* • **needs more info (1)** • **not hacked into a lot (1)** • **third party (11)**: *bad security, good security at company* • **unclear (2)**

C Follow-up Survey Material

C.1 Initial Message To Participants Eligible to Participate In the Follow-Up Survey

You participated in our previous study about people's reactions to data breaches in September/October 2020. We would like to invite you to participate in a follow-up survey as part of our research. The survey will take about ten minutes and you will be compensated $2.50 upon completion. If you are interested, please click <link> to access the survey.

C.2 Informed Consent

Study Title: Follow-up survey on reaction toward data breaches
Principal Investigators: Adam Aviv, Associate Professor, George Washington University
Florian Schaub, Assistant Professor, University of Michigan
Purpose of this Study: We are conducting a research study to understand how users react to data breaches.
Description of your involvement: You participated in our previous study in September/October 2020, in which you reviewed data breach records associated with one of your email addresses based on a public database of data breaches (haveibeenpwned.com).

If you agree to be part of this new study, we will ask you to complete an online survey about your experiences and actions since our previous survey.
Requirements: To participate in the study, you must (1) be 18 years old or older; (2) currently live in the United States; and (3) have participated in our previous study in September/October 2020.

Benefits: You may not receive a direct benefit from participating, but this study will help us develop better technologies that empower Internet users to protect themselves against data breaches.
Risks: The risks and discomfort associated with your participation are not greater than those ordinarily encountered in daily life or during use of the Internet.
Compensation: The survey will take about 10 minutes. You will be compensated $2.50 upon completing this survey.
Confidentiality: By participating in the study, you understand and agree that the University of Michigan and George Washington University 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 and consent form will be kept separate. Your research data will be stored securely and will only be accessible to the study team. You will NOT be asked to provide any direct personal identifiers in the study. Please also avoid disclosing personal identifiers in filling out the survey. The data gathered during this study may be published in an academic journal or conference paper. We will verify anonymity in all survey responses before the publication.
Rights: You can choose to withdraw from this study at any time. To do that, simply close the browser window. We will remove any incomplete survey responses from our records before the analysis. Unfortunately, we cannot provide you with compensation if you choose to opt out. If you have any questions about this study, you may contact the study team by emailing data-breach-hibp@umich.edu.

The University of Michigan Health Sciences and Behavioral Sciences 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. Please be sure we have answered any questions you may have, and you understand what you are being asked to do.

STATEMENT BY PERSON AGREEING TO PARTICIPATE IN THIS STUDY: I have read this informed consent document and the material contained in it. I understand each part of the document, all my questions have been answered, and I freely and voluntarily choose to participate in this study.

C.3 Follow-up Survey Instruments

In our previous study, we used an email address you provided to look up whether your email address has appeared in any data breaches (also called "security breaches"). **Our record shows that your information was part of one or more data breaches.** We'd like to learn about your experiences and behaviors since that study.

(29) Do you remember participating in this previous study? Please answer honestly. Your response to this question will not affect your compensation or ability to participate in this study. [Participants were not screened out based on responses to this questions] ○ Yes ○ No ○ Not sure

Questions about generic actions we provide:

(30) According to our records, you participated in our previous study on <DATE>. In the time since, have you taken any of the following actions? Please answer honestly – we'd like to learn about your actual behavior. Your responses will not affect your compensation for this study. ○ I signed up for a breach notification service (e.g., Firefox Monitor, Breach Clarity, Have I Been Pwned) ○ I signed up for a credit or identity monitoring service (e.g., LifeLock, Identity Guard, IdentityForce, Credit Karma, Credit Sesame) ○ I placed a credit freeze on my credit reports ○ I reviewed my credit reports for suspicious activity ○ I reviewed my bank for suspicious activity ○ I reviewed my credit card statements for suspicious activity. Answer options: ○ Yes – within a week ○ Yes – within a month ○ Yes – after a month or later ○ No – but I plan to do this soon ○ No – and I'm not planning to do this ○ I already did this before the previous study

(a) (*If signed up for credit or identity monitoring services*) You indicated that you signed up for a credit or identity monitoring service. Did you pay for this service or use a free version? ○ I paid for a credit or identity monitoring service. ○ I use a free version of a credit or identity monitoring service. ○ I accidentally selected the wrong answer in the previous page — I did not sign up for a credit or identity monitoring service.

(b) (*If signed up for credit or identity monitoring services*) Which credit or identity monitoring services did you sign up for? ○ LifeLock ○ Identity Guard ○ Credit Karma ○ Credit Sesame ○ Other[free text]

(31) In the previous question you said you took these actions since <DATE>: [Show all action items for which one of the YES options was selected]. Please elaborate on your motivations and experience of taking these actions. [free text]

(32) In the previous question you said you **did not** take these actions since <DATE>:[Show all action items for which one of the No options was selected]. Please explain your reasons for not taking these actions. If you wanted to take some of these actions, what prevented you from doing so? [free text]

Questions about breach-specific actions:

Next, we are going to ask you about actions you might have taken in response to a specific data breach we showed you in our previous study. We will show you the same information about each breach that we showed you last time, before asking you a few questions.

(33) In our previous study, on <DATE>, we informed you that your information was part of this data breach: [Show the breach info]. Since then, have you taken any of the following actions in response to this data breach? If you don't have an account with this company, please select "Not applicable" for questions asking about accounts. Please answer honestly – we'd like to learn about your actual behavior. Your responses will not affect your compensation for this study. ○ I changed the password of my <breach name> account ○ I changed the password of other accounts that used the same password as my <breach name> account ○ I enabled two-factor authentication for my <breach name> account ○ I deleted or deactivated my <breach name> account ○ I filed a complaint against <breach name> with a consumer protection agency (e.g., Federal Trade Commission, Consumer Financial Protection Bureau, State Attorney General) ○ I have taken legal action against <breach name> ○ I warned people I know (e.g., family members, friends, colleagues) about this breach Answer options: ○ Yes – within a week ○ Yes – within a month ○ Yes – after a month or later ○ No – but I plan to do this soon ○ No – and I'm not planning to do this ○ I already did this before the previous study ○ Not applicable

(34) In the previous question you said you took these actions in response to the <breach name> breach since <DATE>: [Show all action items for which one of the YES options was selected]. Please elaborate on your motivations and experience of taking these actions. [free text].

(35) In the previous question you said you **did not** take these actions in response to the <breach name> breach since <DATE>: [Show all action items for which one of the NO options was selected]. Please explain your reasons for not doing so. If you wanted to take some of these actions, what prevented you from completing them? [free text]

Closing Comments:

(36) Have you done anything else we haven't asked about in response to learning that you were affected by data breaches in our prior study on <DATE>? If yes, please describe what you did and why. [free text]

(37) Thank you for your participation! Would you be interested in participating in an optional interview (about 60 minutes long) regarding your experiences with data breaches? The interview will be conducted remotely via Zoom, and you would be compensated $15 for your time through Prolific. If you are interested and are selected for an interview, we will send you a Prolific message to schedule the interview. ○ Yes, I am interested in participating in an interview ○ No, I am not interested in participating in an interview

D Follow-Up Survey Qualitative Codebook

In the following we provide our unified codebook with the primary codes, their respective counts, and their first-level sub-codes.

D.1 Codebook for Q31

• **changed password(5)**: • **concern (17)**: *breach occurence, density of breaches,fraud,identity theft, personal information.* • **conditional awareness(1)**: • **preventative measure (8)**: *credit freeze* • **prior incident(15)**: *data breach, debit card, identity theft, paypal, unauthorized charge* • **reviewed (43)**: *HIBP, accounts, after, bank, bank statement, breach report, credit report, credit statement, prior, regularly, statement,two* • **service (6)**: *LifeLock,breach notification, chrome notification,credit card, credit ID service, credit karma, nerd wallet* • **smart(1)**: • **unconcern (2)**: *too small* • **wants to improve (4)**: *took action*

D.2 Codebook for Q32

• **use service (19)**: *Transunion, Identity theft services, H&R Block, Google Security Feature, Experiean, Credit Karma, Credit Scout, Chase, Bank, Avast* • **Unnecessary (18)**: *Credit Score Good* • **Unmotivated(26)**: *No harm, does not want to take further action, does not want to pay* • **skeptisim (2)**: *security concerns* • **services to expensive(5)**: • **Self-Monitor(10)**: • **Resigned (14**: *Process would be too difficult, poor credit, not interested in improving credit* • **proactive(21)**: *secure passwords, put hold on credit card, changed password, monitors credit, check statements* • **plans to take action(3)**: • **pending transaction(3)**: *mortgage* • **not concerned (8)** • **not an often occurrence (4)** • **not a target (9)** *minimal assets* • **no current issues (11)** • **lack of awareness (10)** • **institutional trust (3)** *banking protections* • **inconvenient(5)** *actively seeking credit* • **forgot(9)** • **credit reports frozen(3)** • **considering other options(3)**

D.3 Codebook for Q34

• **awareness(4)**: *secure passwords, put hold on credit card, changed password, monitors credit, check statements* • **change password(35)**: *after breach, all passwords, frequent use, more frequently, more secure, prevent access, similar passwords, single account* • **concern (2)** • **delete account (3)** • **ease of use (7)** *delete account* • **followed instructions (1)** • **password reuse (7)** • **prevent further risk (1)** *data, privacy information* • **proactive (5)** *identity theft* • **protection (9)** *future breaches* • **necessary action (3)** *safety* • **service (9)** *2FA, google password check, password encryption, password manager* • **share knowledge (19)** *family, friends* • **undescriptive (2)** • **undesire for service (1)** • **unease of use (1)** *unable to contact* • **unused account (25)** *begin resusing, deleted account, might delete* • **used account (6)** *deleted account, low use*

D.4 Codebook for Q35

• **apathy(50)**: *no bad outcome, not a threat, to much risk, unimportant information* • **awareness of threat (4)** • **forgot (4)** • **awareness of threat (4)** • **forgot (20)** • **inactive account (8)** • **inactive email (2)** • **inconvenient (20)** *2FA,account in use, financial* • **inconvenient (20)** *2FA,account in use, financial* • **modified account (25)** *canceled, changed password, deleted data* • **no mutuals(21)** • **not a target(38)** • **not a concerned (21)** • **not willing to take action (15)** *account active* • **proactive measures (10)** *no duplicate passwords, unique passwords* • **resigned (6)** *already breached* • **resigned (6)** *already breached* • **share knowledge (1)** • **technology limitation (1)** • **throw away password (1)** • **unaware of account (31)** • **unaware of action (9)** *take action* • **unknown company (18)** *Appen, Canva, Modern Business Solutions, River City MediaSpam List* • **unknown company (18)** *Appen, Canva, Modern Business Solutions, River City MediaSpam List* • **unnecessary (33)**

E Author Statement

Unique contributions relative to the authors' prior publications. Our manuscript is an extension of a conference paper previously published at the 2021 USENIX Security Symposium. In the original conference publication, we describe the results of an online survey (n=413) in which we presented participants with up to three data breaches that had exposed their email addresses and other personal information. We aimed to answer five research questions regarding the participants' data breach status, perception of data breaches, awareness of data breaches, emotional response, and behavioral response. The results indicated that 73% of participants were affected by at least one breach. Participants were unaware of 74% of displayed breaches and expressed various emotions when learning about them. Many participants attributed the cause of being affected by a breach to their poor email and security practices instead of external factors such as breached organizations and hackers.

As an extension of the work described above, we report on results from a previously unpublished follow-up survey with participants of the main survey (n=104), revisiting the breaches they experienced and the actions they intended to take. The follow-up survey sought to investigate whether there is a gap between participants' intention to act (as measured in the main survey) and actual behavior, as well as the motivators and impediments for participants to follow through with their intention. We identified a sizable intention-behavior gap; the presence of the gap largely depends on the specific action. Participants' motivators for taking action include concern, prior incidents, and a proactive attitude toward security risks. By contrast, participants refrained from following through with their intention when they were apathetic about breaches, considered potential costs, forgot, or felt resigned about taking action. We provide empirical and practical implications based on findings from the follow-up survey, such as developing a better understanding of the (ir)rationality behind inaction and designing interventions that help bridge the identified intention-behavior gap.

Other related work done by some of the authors. Zou et al. qualitatively investigated consumers' mental models of credit bureaus, how they perceive risks from the Equifax data breach, whether they took protective measures, and their reasons for inaction [142]. While this work also reports that individuals were unaware of whether they were affected and might not take action after a breach, the investigation focused on one specific breach and was qualitative in nature. The research presented in this paper instead probed individuals with up to three breaches that affected them. It includes quantitative as well as qualitative findings.

In addition, Zou et al. conducted an analysis of 161 data breach notifications with respect to their readability, structure, risk communication, and presentation of potential actions [141]. The results of this analysis indicate that notifications are long and require advanced reading skills. Many companies use language to downplay or obscure whether the receiver of the message is affected. Moreover, potential actions and offered compensations are frequently described in lengthy paragraphs instead of clearly listed. In light of these findings, we opted for a short description of the breaches in our study. The detailed design of notifications is, however, subject of future work.