Who Would Bob Blame? Factors in Blame Attribution in Cyberattacks Among the Non-adopting Population in the Context of 2FA

Sarah Marie Peck
Department of CSE
University of Connecticut
sarah.peck@uconn.edu

Mohammad Maifi Hasan Khan
Department of CSE
University of Connecticut
maifi.khan@uconn.edu

Md Abdullah Al Fahim
Department of CSE
University of Connecticut
md.fahim@uconn.edu

Emil N Coman
University of Connecticut Health Center
Farmington, CT USA
coman@uchc.edu

Theodore Jensen
Department of CSE
University of Connecticut
theodore.jensen@uconn.edu

Yusuf Albayram
Department of CSE
University of Connecticut
yusufalbayram@gmail.com

***Abstract*—This study focuses on identifying the factors contributing to a sense of personal responsibility that could improve understanding of insecure cybersecurity behavior and guide research toward more effective messaging targeting non-adopting populations. Towards that, we ran a 2(account type)x2(usage scenario)x2(message type) between-group study with 237 United States adult participants on Amazon MTurk, and investigated how the non-adopting population allocates blame, and under what circumstances they blame the end user among the parties who hold responsibility: the software companies holding data, the attackers exposing data, and others. We find users primarily hold service providers accountable for breaches but they feel the same companies should not enforce stronger security policies on users. Results indicate that people do hold end users accountable for their behavior in the event of a breach, especially when the users' behavior affects others. Implications of our findings in risk communication is discussed in the paper.**

***Index Terms*—Cybersecurity; Risk Communication; Blame Attribution**

I. Introduction

Researchers have looked at various factors that may explain and alter users' behavior both in security and privacy contexts such as gaps in mental models, low risk perceptions, cost involved (i.e., time and money), and poor efficacy of message designs [1]–[14].

Risk perception research has shown that people do not adequately understand the risks involved with their data being public, and more education leads to greater risk perception by users [15]–[17]. However, users do not always take recommended action, even when people know what the risk is, what to do about that risk, and how they should act [18], [19]. This suggests that there are other components to encouraging user action beyond education and increasing risk perception. A variety of motivational theories have been proposed and applied to security behavior [20]–[25], but research suggests that a person's sense of responsibility to act could be a valuable addition to those theoretical models [26].

A first step to examining whether a responsibility to act motivates behavior is to determine who is held responsible in the case of a data breach and why. When do users feel that the responsibility for data breaches lies with others? Even though users are directly affected, they may hold other parties accountable on their behalf. Understanding how blame is attributed after a data breach may determine how to approach messaging and encourage more secure behavior. It may also help explain motivational questions in a variety of fields, such as the privacy paradox.

In this paper, we examine which factors contribute to responsibility distribution, and how non-adopting population allocate blame and responsibility and whether messages, account ownership, and usage behavior have an effect on blame distribution. To answer these questions, we designed a 2(account type)x2(usage scenario)x2(message type) between-group study using a factorial set of vignettes and recruited 237 Amazon Mechanical Turk users in the United States aged 18 and above. The surveyed population was split into 8 subgroups, and each group was asked about the vignette protagonists' feelings, motivations, and placement of blame as he made the decision to decline two-step verification protection for his email.

The study finds that users primarily hold the service provider (i.e., Google in our case) accountable for breaches. Interestingly, even though they want those companies to do more to protect their *servers*, they do not feel that the same companies should enforce stronger security policies for users. Survey participants regularly expressed an attitude of "to each their own," sharing a strong belief that users know best what level of security is appropriate for the context in which they use a particular account.

Our findings further suggest that people do hold end users accountable for their behavior in the event of a breach, especially if it harms people who have less control over the

978-1-7281-7303-0/20/$31.00 ©2020 IEEE
DOI 10.1109/COMPSAC48688.2020.0-166

exposed data. Additionally, several responses shared a belief that the end user would pass the blame on to someone else and would not want to hold himself responsible, even if the end user recognized that he had an opportunity to prevent the attack. This indicates a sense of shame and responsibility among users, which may be leveraged to trigger the feeling of responsibility and change in behavior [26]. Details of our study and findings along with broader implications are presented in the paper.

II. Related Work

In the area of usable cybersecurity, how people conceptualize and protect their data is widely studied to help researchers and industry work with users to ensure security and privacy [27]–[29]. In 2009, Herley suggested that failure to adhere to good security behavior could be attributed to users' perceptions of the costs being too high and/or benefits being too low [1], which is supported by more recent work [6]. Further, even when people know what the risk is, what to do about that risk, and how they should act, users do not always take recommended action [18], [19]. Over the years, numerous studies have tried to understand and identify the underlying factors that may explain non-expert users' insecure cyberbehavior in different contexts (ranging from password creation to adoption of security tools and privacy behaviors) [2], [3], [7]–[10], [14].

There are several models for human behavior that attempt to explain this dichotomy. These models often theorize what is necessary for users to take action, but are not always sufficient for action to take place. Among numerous models, we discuss the commonly cited models below.

A. Protection Motivation Theory

A well-known theory that explains how people respond to threats is Rogers' Protection Motivation Theory (PMT) [30]. In this model, to change behavior, one would first expose a threat that the current behavior does not address, and then recommend a protective action to address the threat. This idea is more commonly known as fear appeal. Rogers' theory states that an effective fear appeal balances the following three components: perceived severity, perceived risk, and the efficacy of a protective response. A fourth item, self-efficacy, was added later [20]. PMT is broad enough to apply to fear appeals generally, but has also been specifically used to encourage secure behaviors in several studies. For example, one recent work used fear appeal to persuade users to enable screen locking and successfully convinced about 50% of users in the short-term [31]. While fear appeal is broadly used in cybersecurity and health campaigns, the results have been mixed and the long-term efficacy is unclear [31], [32].

B. Theory of Planned Behavior

An alternate theory proposed by Ajzen [22] is the Theory of Planned Behavior (TPB). This theory states that an individual's behavior can change through the following factors: a positive attitude toward the behavior, subjective norms (people around the individual having a positive attitude toward the behavior), and self-efficacy. Each of these factors have been shown to increase the behavioral intention of compliance with an information systems security policy [23]. However, this model does not explicitly consider the role of self-responsibility in promoting secure behavior.

C. Health Belief Model

The Health Belief Model (HBM) has been found to have a strong fit to Internet security behavior [21], [24]. This model posits that behavior change is based on the following six factors: risk perception, perception of severity, perceived benefits, perceived barriers, cues to action, and self-efficacy [33]–[35]. Ng et. al. shows that each of those six factors impacts computer security behavior, where susceptibility, benefits, and self-efficacy are determinants of behavior [21].

D. Bayesian Economics

In addition to motivational models, there are economic models to explain why users may or may not adopt security tools. However, these models are imperfect because while users may be making rational economic choices for themselves based on perceptions of cost and benefit [1], [6], [36], humans' bounded rationality, imperfect knowledge, and psychological deviations from rationality prevent people from making rational economic decisions at all times [37].

E. Responsibility

The researchers argue that the existing models fail to account for how users allocate blame and responsibility in the event of a data breach, and incorporating the perceived responsibility of different parties in the cybersecurity context could help researchers better understand user behavior. While people hold companies responsible for breaches and there is a cost to a company who is breached, that cost tends to dissipate over time [38]. Personal responsibility may have a role to play in cybersecurity behavior [39]. A study by Yazdanmehr and Wang [26] goes beyond the existing frameworks to explore the effects of several factors on information security policy (ISP) compliance behavior. They show that there are more factors than the current theories incorporate. They write, *"We show that the strength of ISP-related personal norms on ISP compliance depends on the degree to which an employee feels personal responsibility."* In other words, an employee's personal inclination to comply with an ISP is not enough to account for their behavior. Rather, the employee must also feel personal responsibility for the organization's ISP. This finding suggests that users may not feel responsible for their data, and may feel that the responsibility for data breaches lies with others. Even though users are directly affected, they may hold other parties accountable on their behalf. Interestingly, none of the current theories includes all of the factors Yazdanmehr and Wang identified to explain ISP compliance.

Thus, we argue that fear appeal may not be adequate alone to promote sustainable change in behavior, and further research is needed to investigate the concept of blame attribution and self responsibility in the context of cybersecurity.

III. Methodology

The purpose of this study is to investigate who users blame for data breaches and why. While many factors may contribute to data breaches and affect blame distribution, we wanted to focus on a scenario that is preventable if appropriate actions are taken by a user. At the same time, the attack could have been prevented by the service provider as well, making it difficult to attribute blame. Specifically, in our case, the attack was preventable if the user (i.e., Bob) enabled two-step verification for his email account. At the same time, the service provider (i.e., Google) could have forced Bob to use two-step verification and prevented the attack. We also hypothesized that the severity of compromise (i.e., loss of personal vs. other people's data) may influence blame attribution as well.

Finally, we hypothesized that the design of the message used by the service provider (i.e., Google in our study) to promote the security feature may influence blame attribution as well as feature adoption. Specifically, a message that contains fear appeal and risk content is likely to trigger different sets of emotions than a message without fear appeal, and may shift the blame towards Bob as he may appear more negligent for ignoring a stern warning. As such, we used two different messages to evaluate these effects (i.e., one is the message incorporating risk information and graphics depicting a person wearing an eye mask (Figure 1) and the other one is the edited version of the same message excluding the risk component and the image of the person wearing an eye mask (Figure 2)). Note that the messages used in the study were edited to suit the purpose of the study, and may not be the same which are used by Gmail to promote 2-step verification (i.e., messages used by Gmail could be seen at https://www.google.com/landing/2step/ at the time of the study). Further, any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of Google/Gmail.

In our study, we seek to answer the following research questions based on the following study variables: type of email account (official email account vs. personal email account), usage scenario (personal vs. personal and business), and design of the message (with vs. without fear appeal):

RQ1 How does account ownership affect delegation of blame after an attack?

RQ2 How does account usage affect delegation of blame after an attack?

RQ3 How does the design of a notification of a new security feature affect delegation of blame after an attack?

RQ4 How does the risk profile of the situation (e.g., loss of personal information versus loss of other people's information) affect perception of risk?

A. Study Design

To answer these questions, we designed a 2(account type)x2(usage scenario)x2(message type) between-group study using vignettes. These stories were about Bob, a protagonist designed to share habits with survey takers. We restricted our population to people who have not implemented two-step verification (see subsection III-C for enrollment criteria).

The vignettes included both relevant and irrelevant information about how Bob behaves when prompted to implement a security feature. We attempted to make these vignettes as realistic as possible by using Gmail as the platform of choice in this study as this is one of the most widely used email service across the world. Further, we restricted participation to people who use Gmail regularly for important tasks based on self-reported data. Participants were assigned to groups randomly to ensure that any possible bias related to using Gmail was uniformly distributed across groups. After viewing the vignette, the survey then asked participants who Bob would blame (open-ended) and whether various parties (e.g., the data holder, the account manager, the end-user, the company using the data, the government, the attacker, etc.) share any responsibility.

We hypothesize that our factorial design would help answer questions about how changes in the story (including changes in the messages the protagonist sees, the protagonist's "personal risk," and the behavior of the protagonist; see Table I for full details) change the way survey participants allocate blame. We anticipate that people are more likely to blame a protagonist, even if the protagonist acts the way the participants do, than the participants would be to blame themselves. Since media attention rarely focuses on the end user, we determined that it would be interesting to see if people would *ever* blame an end-user, so we determined that the best course of action would be to use vignettes following a neutral protagonist.

Once participants give informed consent and start the study, vignette part 1 is presented, in which Bob's email habits are established and participants see a message encouraging Bob to enable the two-step verification feature for his email. These vignettes are factorial in nature, with two binary variables. Bob's email account is either an official business account or a personal account. Bob either uses the account for personal use or business and personal use. Finally, participants see one of two messages encouraging adoption, one of which is the message incorporating some degree of risk information and fear appeal, and one is an abridged version of the same message. These three factorial variables are evaluated for their impact on participants' distribution of responsibility. The vignettes are presented below.

Vignettes, Part 1, Group 1 - Office email; business and personal use. *Bob works for a health insurance company and the company provides email service to the employees through commercial Gmail service. He uses his official Gmail account for his official and personal business and often exchanges health insurance claim files with his colleagues using the email account. On Dec 7, 2017, he received an email from Google (shown below) promoting a security feature called two-step verification that is supposed to enhance the security of the account and decided not to activate the feature.*

Vignettes, Part 1, Group 2 - Office email; personal use. *Bob works for a health insurance company and the company provides email service to the employees through commercial*

TABLE I: Use case scenarios

Email Account Scenario	Message
Account type: Office email; Usage: Business and personal use	Message with Risk Content (Group 1A) Abridged Message (Group 1B)
Account type: Office email; Usage: Personal use	Message with Risk Content (Group 2A) Abridged Message (Group 2B)
Account type: Personal email; Usage: Business and personal use	Message with Risk Content (Group 3A) Abridged Message (Group 3B)
Account type: Personal email; Usage: Personal use	Message with Risk Content (Group 4A) Abridged Message (Group 4B)

Gmail service. He uses his official Gmail account for his personal business. On Dec 7, 2017, he received an email from Google (shown below) promoting a security feature called two-step verification that is supposed to enhance the security of the account and decided not to activate the feature.

Vignettes, Part 1, Group 3 - Personal email; business and personal use. *Bob works for a health insurance company and uses his personal Gmail account for his official and personal business. He often exchanges health insurance claim files with his colleagues using the email account. On Dec 7, 2017, he received an email from Google (shown below) promoting a security feature called two-step verification that is supposed to enhance the security of the account and decided not to activate the feature.*

Vignettes, Part 1, Group 4 - Personal email; personal use. *Bob works for a health insurance company and uses his personal Gmail account for his personal business. On Dec 7, 2017, he received an email from Google (shown below) promoting a security feature called two-step verification that is supposed to enhance the security of the account and decided not to activate the feature.*

After participants read vignette part 1 and see the message promoting 2FA, they are then told that Bob chooses not to enable the feature, and are asked questions about the reasons Bob presumably chose not to enable the feature. After that, a follow-up to the vignette (i.e., Follow-up vignette) is then shown in which Bob's email is breached in a way that could have been prevented if he had used two-step verification. The true cause of the breach is not clear to participants to keep the situation as general as possible. The vignette is as follows.

Follow-Up Vignette. *On Dec 7, 2017, Bob decided not to activate two-step verification. On Dec 15, 2017, security attackers broke into the Google authentication server and stole login credentials of several thousand users. However, Bob was unaware of the attack as Google did not identify the attack immediately and failed to notify the users. On Dec 20, 2017, the attacker used the stolen credentials from the social media account to log into his email account and then changed the password, preventing him from accessing his own email account.*

After viewing the follow-up vignette, participants are then asked who Bob would hold responsible for the breach and why. Finally, participants are asked for demographic information.

Overall, the survey took participants about a half an hour to complete (median = 29.57 minutes, mean = 35.18 minutes, SD = 23.28 minutes, one outlier removed). Participants were paid $3 on Mechanical Turk for taking this survey. The survey and methodology for this study were approved under an exempt protocol by the IRB of the University of Connecticut.

B. Measurement

The survey questions are mostly in the form of agreement to a statement on a 5-point Likert scale [40] and open-ended questions about why participants chose their response. The survey included specific questions like "Who would Bob blame?" as well as questions about how other parties in the scenario should have behaved by asking participants how much they agreed with statements like "Enabling two-step verification can inconvenience the owner of the email account." The survey also asked participants to explain their thinking to expose the reasoning behind their decisions. The research questions were answered by comparing responses to questions between groups to determine significant differences, and then relating those differences back to respondents' thinking.

C. Participant Population

Participants were recruited using Amazon's Mechanical Turk (MTurk) platform. We restricted participants to those 18 years of age or older, currently living in the United States, having completed at least 1000 HITs (Human Intelligence Tasks), and having a HIT approval rate greater than 95%, which is recommended by prior work [41]. While MTurk participants may not be statistically representative of the adult population in the United States, they are still noted to be more representative than other convenience samples [42] and MTurk's use has been noted in numerous prior efforts [43]–[46]. The participants must meet the following criteria to be eligible for the study:

- Be proficient in English
- Not have a degree in Computer Science, including a "minor" or any professional computer science certifications
- Not a user of two-factor authentication
- Use a Microsoft Windows computer
- Use Gmail

The population we focus on is the population of users without expertise in computers or security, but who use technology proficiently enough to be at a significant risk for security vulnerabilities. We focus primarily on those not using all of the security tools available to them, so the participants were restricted to those who do not use two-factor authentication already. To ensure a uniform baseline, we also chose to restrict our population to just Windows users because of widespread existing notions about relative security of different operating systems [47], [48]. Not having extensive formal education in computer science was required because previous studies have shown that more knowledge of security issues increases risk perception [15]–[17]. Proficiency in English was mandatory because the survey was conducted and evaluated in English.

Fig. 1: Message with Risk Content

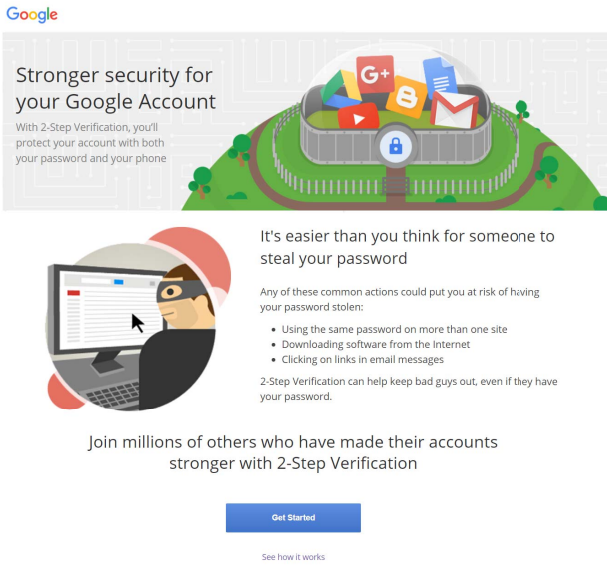
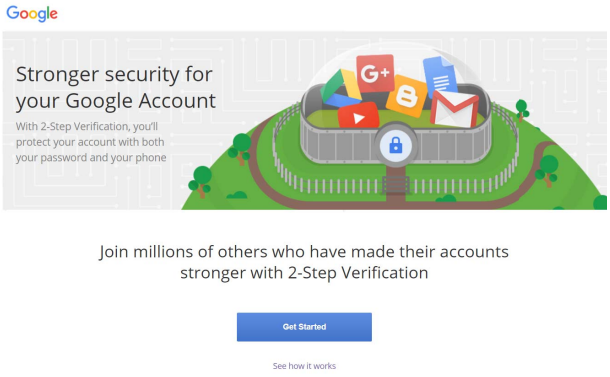


Fig. 2: Abridged Message



The participants were randomly separated into eight distinct groups, as highlighted above. Participants were kept anonymous and questions were ordered to minimize biasing.

D. Data Analysis

The survey consisted of both qualitative and quantitative questions inspired by prior work [6]. The quantitative questions were evaluated with UNIANOVA processing to compare responses across the vignette scenarios and find factors explaining the variability in responses.

A confidence interval of 95% was used on the data. To test the assumption of equal variance, a Levene test was run before UNIANOVA processing. If the Levene test indicated that the assumption of equal variance was violated, the p-value was reduced to 0.01 before results were considered significant. We also tested differences between normal ANOVA assuming normality and corrected ANOVA models (the ANOVA-type statistic and the Wald-type statistic), because of the potential for the distribution of model residuals to fail the normality assumption. As fewer than 1% of results changed in their conclusion (in terms of significance), we report the unadjusted results. Analyses were done in SPSS and R [49]–[51].

Data was cleaned prior to statistical evaluation. Responses to attention-check questions were used to filter out responses that were potentially unreliable. Mechanical Turk's tools to prevent the same user from responding multiple times were used. To further eliminate the possibility of duplicate participation, respondents who submitted answers that were exact or very close duplicates of other narrative answers were removed. In this way, 15 of the 252 responses (6.0%) were removed from the data.

We used a bottom-up inductive coding approach [52] at the question level in order to code responses to the open-ended questions. Initially, two researchers worked independently and read through all the comments and developed a set of codes for each question. These two coders then met to discuss and create the final codebook for each question. Once the codebooks were finalized, the two coders updated their codebook independently. Inter-rater reliability was calculated for each question using Cohen's Kappa which ranged from 0.76 to 0.95, indicating "substantial" or "excellent" agreement between the coders [53]. See Tables II, III, IV and V for codes and question-specific inter-rater reliability. The details are presented below.

IV. Evaluation

A. Demographics

Overall, this study included 237 valid responses. Ages ranged from 20 to 69 years old (mean = 35.6, SD = 10.6). This population was made up of 138 males (58.2%), 96 females (40.5%), 2 other and one participant who preferred not to answer. Race was not recorded. See Table VI for the demographic breakdown of each group.

A Chi-squared test revealed no significant differences between groups in terms of gender ($\chi^2(21) = 15.25 p = 0.81$). A Kruskal-Wallis test found no significant differences between groups in terms of age ($\chi^2(7) = 2.08, p = 0.96$) or in terms of time spent taking the survey ($\chi^2(7) = 4.777, p = 0.687$). The researchers conclude that the groups are demographically similar and can be compared.

TABLE II: Codes for "Why do you think Bob declined to enable two-step verification? Please explain." ($\kappa = 0.87$)

Code	1A	1B	2A	2B	3A	3B	4A	4B	Total
Enabling takes too much effort	52%	67%	56%	41%	57%	46%	63%	50%	53%
Enabling takes too much time	22%	29%	20%	16%	11%	23%	20%	17%	19%
Did not know what would happen	26%	33%	32%	24%	29%	27%	27%	37%	29%
Did not need extra protection	17%	13%	36%	38%	37%	38%	27%	37%	31%
I do not know	0%	0%	0%	0%	0%	0%	3%	0%	0%
Unable to code	13%	0%	16%	3%	9%	8%	0%	17%	8%
Number of valid responses	23	24	25	37	35	26	30	30	230

TABLE III: Codes for agreement with the statement "Google did the right thing by not forcing Bob to enable two-step verification. Please explain the reasoning behind your answer." ($\kappa = 0.80$)

Code	1A	1B	2A	2B	3A	3B	4A	4B	Total
Two-step verification is untrustworthy	0%	0%	0%	0%	3%	0%	0%	0%	0%
Two-step verification is inconvenient	8%	0%	12%	11%	16%	7%	7%	16%	9%
It should be Bob's choice	92%	91%	92%	62%	80%	78%	86%	94%	83%
Google should force to avoid consequences to itself	0%	9%	4%	8%	6%	0%	3%	0%	4%
Google should force for Bob's own good	4%	9%	0%	5%	11%	11%	3%	0%	6%
Bob should still enable	8%	0%	0%	11%	3%	4%	3%	0%	4%
I do not know	4%	4%	0%	3%	0%	7%	3%	3%	3%
Other	0%	0%	0%	5%	0%	0%	3%	0%	1%
Unable to code	4%	4%	16%	0%	9%	4%	3%	9%	6%
Number of valid responses	26	23	25	37	35	27	29	32	234

TABLE IV: Codes for agreement with the statement "Bob did the right thing by not enabling two-step verification. Please explain the reasoning behind your answer." ($\kappa = 0.76$)

Code	1A	1B	2A	2B	3A	3B	4A	4B	Total
It is Bob's decision to make	21%	29%	9%	30%	9%	14%	50%	22%	23%
Two-step verification is untrustworthy	4%	0%	0%	0%	3%	0%	4%	3%	2%
Two-step verification is unnecessary	0%	0%	0%	3%	0%	11%	15%	0%	4%
Two-step verification is inconvenient	0%	0%	0%	0%	12%	4%	15%	19%	7%
Bob should consider other people's data	13%	17%	9%	3%	6%	21%	0%	0%	8%
Two-step verification is beneficial	67%	58%	74%	49%	76%	61%	38%	69%	61%
The account is valuable	17%	13%	26%	19%	40%	25%	8%	28%	22%
I do not know	8%	13%	0%	3%	6%	11%	4%	6%	6%
Unable to code	13%	0%	26%	5%	12%	0%	15%	13%	10%
Number of valid responses	24	24	23	37	33	28	26	32	227

TABLE V: Codes for "Who do you think Bob would blame for the attack and why?" ($\kappa = 0.95$)

Code	1A	1B	2A	2B	3A	3B	4A	4B	Total
Hackers	33%	39%	29%	24%	35%	19%	34%	3%	30%
Google	46%	61%	50%	52%	65%	77%	72%	70%	62%
Himself	50%	26%	50%	27%	50%	35%	38%	43%	40%
No one	0%	0%	8%	0%	6%	0%	3%	0%	2%
The internet in general	0%	4%	0%	3%	3%	0%	0%	0%	1%
I do not know	4%	0%	0%	0%	0%	0%	0%	0%	0%
Other	0%	0%	0%	3%	0%	0%	0%	0%	0%
Unable to code	13%	4%	17%	3%	12%	8%	3%	17%	9%
Number of valid responses	24	23	24	37	34	26	29	30	227

TABLE VI: Participant Demographics by Group

Group	Number of Valid Responses	Age			Gender Breakdown
		Mean	Median	Std. Dev.	
1A	25	36.3	34.0	9.4	13 Male, 12 Female
1B	24	36.0	32.0	13.6	15 Male, 8 Female, 1 Other
2A	28	34.2	33.5	7.2	16 Male, 11 Female, 1 Other
2B	32	37.5	36.0	12.9	19 Male, 12 Female, 1 Prefer not to answer
3A	32	36.3	32.5	10.6	23 Male, 15 Female
3B	27	35.0	33.0	9.3	14 Male, 13 Female
4A	30	35.1	32.5	11.3	18 Male, 12 Female
4B	33	34.3	31.0	9.9	20 Male, 13 Female

B. Users' Response to Negligent Behavior: Before the Attack

1) Should Google Force Adoption?: Participants answered several questions about the relationship between Google's responsibility to push the two-step verification feature and Bob's responsibility to adopt that feature. Overall, participants indicated strong agreement that "Google did the right thing by not forcing Bob to enable two-step verification," with 80.6% of participants who responded either somewhat or strongly agreeing with the statement. 4 participants declined to answer the question. This result is consistent with a later question asking for agreement with "Google should not have asked and should have automatically enabled the two-step verification feature," where 72.0% of responding participants indicated disagreement.

In both of these questions, the vignettes participants began with significantly affected the results. Participants responding to "Google did the right thing by not forcing Bob to enable two-step verification" were significantly more likely to agree if the account was Bob's personal account than if it was an official business account ($F(1,227) = 7.51, p < 0.05$; Cohen's $d = 0.38$), although the effect size was not very large.

Among participants responding to "Google should not have asked and should have automatically enabled the 2FA feature," there was a significant interaction effect between account type and usage. When Bob is using his email for personal purposes, participants feel Google has more authority to force adoption when the account is an official business account than when it is a personal account ($F(1,120) = 8.44, p < 0.01$ (failed Levene test of homogeneity of variance); Cohen's $d = 0.52$).

Responses like "to each their own" and "You can't force anyone to do anything" were common and appeared as reasons for participants' agreement with, for example, "Bob did the right thing by not enabling two-step verification." 83.3% of responses to the statement "Google did the right thing by not forcing Bob to enable two-step verification" included this sentiment.

> *Google does not need to force people to do anything. They tell them what they think is right, but it is the American way to let people make their own decisions.*

This response reflects a belief that consumers should be able to make independent choices and take on risk themselves. The respondent also appears to believe that this is an American perspective. This raises a further question for study: Is blame distributed differently in different cultures? If it is, interventions may need to be tailored to the context in which they are used. Further investigation is needed to answer this question.

While this response was very common, there was still a subset of dissenters, about 5.6% across groups, who felt that Google should enforce adoption for the good of the user. One respondent wrote:

> *Actually, in my opinion, Google should make this 2-step verification process a standard feature of their service if it really provides enhanced security. The best security available should be standard, not optional, as far as I'm concerned.*

This is fairly representative of the reasoning behind responses encouraging Google to have the best security available on by default for the good of the user. There was even a subset of users (3.8%) who believed Google should force users to adopt two-step verification for the sake of Google's well-being rather than the sake of users.

2) Should Bob Have Enabled Two-Step Verification?: When the email account was official, participants were more likely to agree that "Bob should have enabled 2FA once he knew about it" ($F(1,227) = 10.13, p < 0.01$ (failed Levene test of homogeneity of variance); Cohen's $d = 0.36$) and that "Bob should have tried to learn more about 2FA before deciding not to adopt it" ($F(1,229) = 10.07, p < 0.05$; Cohen's $d = 0.39$). Patterns in the data suggest that participants expect Bob to adopt more security features with an official company email account than with his own, regardless of usage.

This research was designed to determine whether Bob had a greater responsibility to secure himself because he had access to other peoples' data. One participant disagreed that Bob did the right thing by not enabling two-step verification, explaining:

> *Especially given that Bob is using his personal email for his work and that it has other peoples info, he should do everything he can to make sure the other peoples info is secure.*[*sic*]

This response indicates that since Bob's account holds other people's data, he has a greater responsibility to protect that data. A corollary, then, is that when Bob is dealing with his

own data, it is more acceptable for him to take risks with that data. If other people would bear the negative consequences of a breach, though, Bob needs to be more secure.

Five participants shared concerns with the security involved with using a two-step verification system. Specifically, they shared concerns with the service provider gaining access to Bob's phone number, as well as the possibility that the email Bob received was actually a phishing attempt. To explain why Bob declined to enable two-step verification, one respondent wrote:

> *Perhaps he doesn't trust the security feature, like he is ignorant to the benefits. He may not have trusted the source of the email. Since hackers have been know to craft fake emails, perhaps Bob was afraid he was being tricked.*

This response also offers insight into the possible intersection of knowledge and trust. That Bob would trust the service more if he understood the benefits of the feature raises a question of whether there exists a relationship between depth of knowledge about a feature and adoption of that feature. In this case and the case where Bob is afraid to share his cell phone number with the system, participants are also questioning the motivation of the two-step verification provider. This comment implies that for optimal feature adoption among this group of participants, both the feature and the company offering the feature would need to be trusted by the adopter.

Some participants take this one step further, as seen in this response:

> *I personally don't trust huge companies who want us to verify identity. It's never to our advantage and it's always to theirs. It doesn't change anything to protect important files and I would have done the same had I been in Bob's place.*

There are other reasons not to enable two-step verification. One participant, for instance, indicated discomfort relying on cell phone service for access to important information:

> *Probably the same reason I have; because I don't want to bother with my cell phone since I live outside of a small town where my cell signal is weak and very unreliable. I am lucky to receive text messages on a good day.*

While the research questions specifically investigated the role of account type, account usage, and messaging on blame distribution, the question of feasibility of parties incorporating stronger security behaviors was not included and could be interesting for future research.

3) The Effect of Intervention Message on Cost-Benefit Analysis: The effect of messaging was different in different contexts. Generally, when the account and usage was personal, the abridged message performed better. Once the email was involved in business, the message incorporating risk content was more effective. For example, when asked how much they agreed with the statement "Enabling two-step verification is beneficial for society," participants responding to personal contexts in which both the usage and account is personal agreed more when they had seen the abridged message than when they saw the message with risk content ($F(1,60) = 15.76, p < 0.05$; Cohen's $d = 1.01$). In the case where Bob is using his personal account for both business and personal purposes, participants who viewed the message incorporating risk content agreed more than participants who viewed the abridged message ($F(1,66) = 21.83, p < 0.05$; Cohen's $d = 1.14$).

Similarly, when agreeing with the statement "Enabling two-step verification can inconvenience the owner of the email account," participants who viewed the abridged message felt that two-step verification was more inconvenient for personal accounts than for business accounts ($F(1,108) = 10.88, p < 0.01$ (failed Levene test of homogeneity of variance); Cohen's $d = 0.63$). When Bob uses a personal account, participants viewing the abridged message also felt it was more inconvenient than participants viewing the message incorporating risk content ($F\ (1,121) = 10.09, p < 0.01$ (failed Levene test of homogeneity of variance); Cohen's $d = 0.59$).

C. Users' Reactions: After the Attack

1) What Worries Bob After an Attack?: Responses indicate that Bob would experience a substantial amount of fear and anxiety after the attack. Participants indicated that Bob is likely to be extremely worried about not knowing what other online accounts may have been affected (81.6% somewhat or strongly agree), that Bob is likely to be extremely worried about not knowing how this may affect others (74.8% somewhat or strongly agree), that Bob is likely to be extremely worried about not knowing what to do next (78.6% somewhat or strongly agree), and that he is likely to be worried about how this may affect himself (82.3% somewhat or strongly agree).

The degree to which Bob would be worried about how this would affect himself is significantly different between a personal and a company account when Bob uses email for personal purposes, and participants agreed more strongly when the account was Bob's personal email ($F(1,138) = 7.5337, p < 0.01$ (failed Levene test of homogeneity of variance); Cohen's $d = 0.46$). This is somewhat inconsistent with participants' written responses that often imply that data has greater value when it is business-related.

2) Who Does Bob Blame?: One participant pointed out Google's responsibility to others in this response regarding who Bob would blame for the attack:

> *He would probably blame Gmail because he would feel Google is one of the biggest Internet companies and they should know how to keep hackers out of their account by now considering hacks would affect people around the world.*

In this example, it appears that the number of people affected would predict a party's responsibility to act securely. This comment indicates that responsibility to protect other people's data applies to both individuals and corporations. The second part of the comment also shows that the greater the reach of a potential data breach, the more resources are expected to be used to protect data.

Another participant who claimed that Bob would blame Google for the attack mentioned Google's resources as justification:

> *I think he'd blame both himself and Google and probably put a little more of the blame on Google since they shouldn't let hackers steal a bunch of data. They have the money and resources to better protect that stuff.*

Several responses also brought up the intersection of personal and business purposes that Bob uses the email account for. This implies that people use different levels of security for different perceived levels of data value. While the survey asked users if they had implemented two-step verification on their own, it is unclear whether participants have ever used two-factor verification in other parts of their lives. One participant felt that Bob did not do the right thing when he chose not to enable two-step verification:

> *I believe it is an important security feature for someone using their personal account for both home and work. Especially someone in the insurance field.*

When asked who Bob would blame for the attack, respondents indicated that while Bob bears some responsibility, Bob would "pass the buck" and blame others instead. One participant shared this sentiment:

> *Bob should blame himself, but it could be that he blames the IT office or a former boss. When it comes to mistakes like this in the workplace, the person should own up to it, but there a several cases where somebody passes the blame to everyone.* [*sic*]

A further response dives deeper into the emotions Bob might feel:

> *I think he may feel ashamed that he didn't do the 2 step verification, and not want to admit that, so he would blame the people responsible for the security attack (the hackers), or maybe even Google itself for not being secure even though they gave him the opportunity to do the 2 step verification.*

Another respondent shares a flawed understanding of the hack as a response for why Bob is not to blame:

> *I think Bob would mostly blame Google for the attack. It wasn't his account specifically which was hacked, but instead it was the Google's servers. Had Google protected their own servers better, the hackers would not have been able to access his account.*

This explanation oversimplifies the vignette scenario and demonstrates a misunderstanding of the purpose of two-step verification technology and how the hackers access Bob's account. Overall, those surveyed felt Bob should try harder to secure his business account than his personal account. Further study is needed to identify the underlying reasons behind such opinions.

3) Changes to Motivational Predictors: The Health Belief Model (HBM) of behavior lists several factors leading to behavioral change, including risk perception, severity perception, perceived benefits and perceived barriers [33]–[35]. We hypothesized that the contextual differences between groups would lead to changes in these factors, as measured by questions in the survey. To determine a change in perceived cost in terms of inconvenience, the participants answered the question "How difficult is it to enable two-step verification?" There were no significant differences between groups for this question. 22.4% of respondents responded that they did not know how difficult it was to implement two-step verification. This is not surprising given that none of the messages shows how to enable two-step verification.

To determine a change in perceived vulnerability or risk, the participants answered these questions: "How vulnerable is your Gmail account without two-step verification?"; "How likely is it for your Gmail account to get compromised?"; "How worried are you about your Gmail account's security?"; and "How concerned are you about your Gmail account being accessed by others?"

Responses to "How likely is it for your Gmail account to get compromised?" were significantly impacted by which message the participant saw, where the message incorporating risk content resulted in an elevated concern over the abridged message ($F(1,229) = 4.43, p < 0.05$; Cohen's $d = 0.26$). Responses to "How worried are you about your Gmail account's security?" were significantly different when Bob is using email for personal purposes. Participants who see Bob using a personal account indicated more worry than when Bob was using an official account ($F(1,121) = 10.27, p < 0.05$; Cohen's $d = 0.58$).

Responses to "How concerned are you about your Gmail account being accessed by others?" were significantly different across groups in three ways. In the case of a personal account and the message incorporating risk content, the scenario where Bob uses email for both business and personal purposes elicited greater concern than when Bob uses email for personal purposes ($F(1,66) = 10.56, p < 0.05$; Cohen's $d = 0.81$).

In the case where Bob uses his personal account for personal purposes, the abridged message generates a greater concern than the message incorporating risk content ($F(1,61) = 10.96, p < 0.05$; Cohen's $d = 0.84$). Finally, when participants see the message with risk content and Bob uses email for personal purposes, the scenario where Bob is using an official account generates more concern than when Bob is using his personal account ($F(1,56) = 11.20, p < 0.05$; Cohen's $d = 0.88$).

To determine a change in perceived severity, the participants answered "If your Gmail account is compromised, how disruptive will this be to your daily life?" There were no statistically significant differences between groups in response to this question.

Overall, the contextual differences in these scenarios did affect participants' responses to measures of factors that HBM predicts will lead to behavior change. Most of the measures above showed that in official contexts or contexts where other people's data are involved, perceptions of risk and severity

increased. However, under very specific circumstances, using the abridged message increased risk perception. In many cases, the context did not have a significant effect. Further studies are needed to understand the interaction effects across multiple factors that may affect risk perceptions.

V. Discussion

While there have been extensive efforts in academia and industry to encourage adoption of more secure behavior among users, users still behave insecurely by reusing passwords, delaying software updates, and not adopting two-step verification when it is made available to them [31], [54]. Some users behave in accordance with their stated beliefs about privacy and protection, while others find the price of marginal protection, in the form of mild inconvenience, too high. This means that there is opportunity and interest in understanding user motivation and decision process around security choices.

Existing motivational theories explain some, but not all, of the factors that change behavior, as Yazdanmehr and Wang show [26]. They demonstrate that a feeling of personal responsibility made a significant impact on behavior change in the workplace. Our study attempts to determine whether some people behave insecurely because they feel that someone else is responsible for protecting their data. To answer that question, researchers started by determining who is held responsible for data and why. The study shows that service providers are largely held responsible for any data breaches, more so than any other party. However, there are circumstances that nudge responsibility back toward the user.

Overall, Google, as the service provider, took the majority of the blame in this survey, but context did play an important role. As the party with the most data, resources, and impact, it is not surprising that it took the brunt of the blame. Though respondents expressed that Bob acted insecurely and had opportunities to be more responsible, he did not carry as much of the blame in the end.

It appears that the degree of influence a party has over securing the data determines the amount of responsibility that party has to protect it. For example, when Google is storing data in a repository, users have very little control over it. This could explain why people do not seem to mind Bob behaving insecurely with his data, but they feel much more opposed to Bob being irresponsible when he has access to other people's data, essentially acting as a proxy data aggregator in participants' mind.

That being said, the circumstances of Bob's situation did have an effect on who is held responsible.

A. Account

When official accounts are being used, the user is held to a higher expectation of personal security conduct. Participants in the study opined that Bob should have learned more before deciding not to adopt two-step verification than when the circumstances were personal. In this case, Bob faces some social disapproval from participants.

However, Bob is still not held to the same level of responsibility as the service provider, which could explain some of the discrepancy in the security paradox. Why would Bob separate his email account uses if he wouldn't get credit for it? A follow-up investigation into blame distribution when Bob is either a secure or insecure user instead of a more typical user could clarify the social incentives behind responsible behavior for users.

B. Usage

Bob's usage of his account affected how blame was distributed. Specifically, when Bob was using his own account for his own purposes, participants were less likely to agree that Bob should have enabled two-step verification early or that he should have tried to learn more before choosing not to adopt the feature. When Bob explicitly mixes purposes within a single account, he is exercising greater freedom and judgment over his email usage. Respondents expect a corresponding rise in responsible behavior when Bob is behaving in ways that are not socially beneficial. When participants mentioned that Bob had a responsibility to others, they blamed him for not behaving more securely.

This finding has wider implications for designing security interventions. For instance, service providers (e.g., Google) can attempt to identify such usage scenarios and deliver personalized security notifications, which are likely to be more effective than a generic message.

C. Design of the Message

Message design had a more nuanced impact on participants' perception of responsibility. Most of the impact of messaging was related to feelings around security instead of directly consequential to blame distribution. The messaging did change the degree to which participants felt that two-step verification is beneficial for society, but the impact was more frequently seen as an interaction effect with the context around Bob's account and usage habits. The data suggest that for personal contexts, the message with risk content was no more effective, and in some cases less effective, than the abridged message. However, participants who viewed the abridged message did indicate that Google could have had a stronger message than participants who viewed the message with risk content. Future research should examine more nuanced intersections of context and messaging.

D. Limitations

Our study suggests that users' do not attribute blame mindlessly, and appears to be affected when others are harmed by their (in)actions. This is in line with prior efforts that showed that social motivations are stronger regulator of behavior than instrumental motivations (i.e., motivations related towards gaining material reward or avoiding material cost) [55]–[57]. Furthermore, the efficacy of risk communication messages can be affected depending on who is at risk. As such, we suggest future studies on message designs incorporating social motives in this context.

However, as with all studies, this study has limitations worth considering. In order to maximize the value of the data collected, we chose to limit the group of participants to adults in the United States with at least the level of technical expertise to use Mechanical Turk. While this population is a relatively good sample for the people most likely to encounter two-step verification messages in the wild, it is not representative of the United States as a whole. The authors attempted to make the situations as realistic as possible, but to make the contexts comparable, some small liberties have to be made. One example is allowing Bob to make security decisions for his business account when in reality, that decision may be made by someone else. Also, people are often more likely to blame someone else than they are to blame themselves. Participants incorporated this belief into their answers, claiming that Bob would pass the blame to another party instead of taking the responsibility himself. It is unclear how the results presented here could be applied to users blaming themselves instead of other users.

Furthermore, to maximize the observed effect, one of the key recommendations in using vignette is to increase the realism by making the experimental settings as similar as possible to the natural settings [58]–[60]. For that, while we considered using an unnamed or generic service provider name instead of Gmail, that had the risk of making the vignettes less relatable, and may not prompt sincere response. As such, to maximize the observed effect, we used Gmail and ensured that only users with Gmail account are allowed to participate. However, to minimize participants' possible personal bias to Gmail (which was unavoidable for the sake of realism), we used Bob instead of asking them to imagine themselves in that situation [61]. Looking at other populations within a corporation (e.g., university campus, Facebook), who will have bias against/for the corporation as well, and comparing their blame distribution would be an interesting follow up study to compare against our findings.

VI. Conclusions

This study builds upon prior research into motivational theories by examining the role responsibility could play in efficacy of risk communication messages. Overall, the participants in this study feel strongly that individual users have the right to make secure and insecure decisions, even when the choice could affect other people. However, when that data does involve others, participants felt less strongly that security interference was inappropriate. While messaging can have an effect on the distribution of blame, its effect appears to be weaker than the effects of account ownership and responsible account usage. Our study underscores the importance of considering social motives while investigating risk communication messages going forward.

VII. Acknowledgments

This research was supported by a NSF CAREER award to the second author, 1750908.

References

[1] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, ser. NSPW '09. New York, NY, USA: ACM, 2009, pp. 133–144.

[2] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""my data just goes everywhere:" user mental models of the internet and implications for privacy and security," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 39–52.

[3] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "" i added'!'at the end to make it secure": Observing password creation in the lab," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 123–140.

[4] E. M. Redmiles, E. Liu, and M. L. Mazurek, "You want me to do what? a design study of two-factor authentication messages," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, Jul. 2017.

[5] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. Washington, D.C.: USENIX, 2013, pp. 257–272.

[6] M. Fagan and M. M. H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016, pp. 59–75.

[7] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri, "Bridging the gap in computer security warnings: A mental model approach," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 18–26, 2010.

[8] A. Woodruff, V. Pihur, S. Consolvo, L. Brandimarte, and A. Acquisti, "Would a privacy fundamentalist sell their {DNA} for $1000... if nothing bad happened as a result? the westin categories, behavioral intentions, and consequences," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 1–18.

[9] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 309–325.

[10] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 213–230.

[11] Y. Albayram, M. M. H. Khan, and M. Fagan, "A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa)," *International Journal of Human–Computer Interaction*, vol. 33, no. 11, pp. 927–942, 2017.

[12] Y. Zou, S. Danino, K. Sun, and F. Schaub, "You might'be affected: An empirical analysis of readability and usability issues in data breach notifications," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, p. 194.

[13] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of ssl warning effectiveness." in *USENIX security symposium*. Montreal, Canada, 2009, pp. 399–416.

[14] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why doesn't jane protect her privacy?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2014, pp. 244–262.

[15] M. W. Skirpan, T. Yeh, and C. Fiesler, "What's at Stake: Characterizing Risk Perceptions of Emerging Technologies," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. 70.

[16] F. Raja, K. Hawkey, S. Hsu, K.-L. Wang, and K. Beznosov, "Promoting a physical security mental model for personal firewall warnings," in *CHI'11 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2011, pp. 1585–1590.

[17] R. Y. Wong, D. K. Mulligan, and J. Chuang, "Using science fiction texts to surface user reflections on privacy," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*. ACM, 2017, pp. 213–216.

[18] Y. Zou and F. Schaub, "Concern But No Action: Consumers' Reactions to the Equifax Data Breach," in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. LBW506.

[19] A. Gambino, J. Kim, S. S. Sundar, J. Ge, and M. B. Rosson, "User disbelief in privacy paradox: heuristics that determine disclosure," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2016, pp. 2837–2843.

[20] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, 1983.

[21] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, 2009.

[22] I. Ajzen, "The theory of planned behavior," *Organizational behavior and human decision processes*, vol. 50, no. 2, pp. 179–211, 1991.

[23] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, pp. 83–95, 2012.

[24] E. E. Jung, E. Y. Ho, H. Chung, and M. Sinclair, "Perceived Risk and Self-Efficacy Regarding Internet Security in a Marginalized Community," *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '15*, pp. 1085–1090, 2015.

[25] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. Menlo Park, CA: USENIX Association, Jul. 2014, pp. 89–104.

[26] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," *Decision Support Systems*, vol. 92, pp. 36–46, 2016.

[27] M. A. DeVito, J. Birnholtz, J. T. Hancock, M. French, and S. Liu, "How People Form Folk Theories of Social Media Feeds and What It Means for How We Study Self-Presentation," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. 120.

[28] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner, "Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 6412–6424.

[29] A. Forte, N. Andalibi, and R. Greenstadt, "Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians." in *CSCW*, 2017, pp. 1800–1811.

[30] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology*, 1975.

[31] Y. Albayram, M. M. H. Khan, T. Jensen, and N. Nguyen, ""...better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, 2017, pp. 49–63.

[32] R. A. Ruiter, C. Abraham, and G. Kok, "Scary warnings and rational precautions: A review of the psychology of fear appeals," *Psychology and Health*, vol. 16, no. 6, pp. 613–630, 2001.

[33] I. M. Rosenstock, "Historical origins of the health belief model," *Health education monographs*, vol. 2, no. 4, pp. 328–335, 1974.

[34] N. K. Janz and M. H. Becker, "The health belief model: A decade later," *Health education quarterly*, vol. 11, no. 1, pp. 1–47, 1984.

[35] I. M. Rosenstock, V. J. Strecher, and M. H. Becker, "Social learning theory and the health belief model," *Health education quarterly*, vol. 15, no. 2, pp. 175–183, 1988.

[36] E. M. Redmiles, M. L. Mazurek, and J. P. Dickerson, "Dancing pigs or externalities?: Measuring the rationality of security decisions," in *Proceedings of the 2018 ACM Conference on Economics and Computation*, ser. EC '18. New York, NY, USA: ACM, 2018, pp. 215–232.

[37] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE security & privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[38] A. Acquisti, A. Friedman, and R. Telang, "Is there a cost to privacy breaches? an event study," *ICIS 2006 Proceedings*, p. 94, 2006.

[39] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, ""my religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking," in *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2657–2666.

[40] R. Likert, "A technique for the measurement of attitudes." *Archives of psychology*, 1932, https://psycnet.apa.org/record/1933-01885-001.

[41] H.-y. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Computers & Security*, vol. 59, pp. 138–150, 2016.

[42] A. J. Berinsky, G. A. Huber, and G. S. Lenz, "Evaluating online labor markets for experimental research: Amazon.com's mechanical turk," *Political Analysis*, vol. 20, no. 3, 2012.

[43] M. Buhrmester, T. Kwang, and S. D. Gosling, "Amazon's mechanical turk: A new source of inexpensive, yet high-quality, data?" *Perspectives on Psychological Science*, vol. 6, no. 1, p. 3–5, Jan 2011.

[44] F. Teschner and H. Gimpel, "Crowd labor markets as platform for group decision and negotiation research: A comparison to laboratory experiments," *Group Decision and Negotiation*, vol. 27, no. 2, p. 197–214, Apr 2018.

[45] G. Paolacci, J. Chandler, and P. Ipeirotis, "Running experiments on amazon mechanical turk," *Judgment and Decision Making*, vol. 5, no. 5, p. 411–419, 2010.

[46] D. G. Rand, "The promise of mechanical turk: How online labor markets can help theorists run behavioral experiments," *Journal of Theoretical Biology*, vol. 299, p. 172–179, Apr 2012.

[47] A. J. O'Donnell, "When malware attacks (anything but windows)," *IEEE Security & Privacy*, vol. 6, no. 3, pp. 68–70, 2008.

[48] M. Lindorfer, B. Miller, M. Neugschwandtner, and C. Platzer, "Take a bite-finding the worm in the apple," in *2013 9th International Conference on Information, Communications & Signal Processing*. IEEE, 2013, pp. 1–5.

[49] H. Wickham and E. Miller, *haven: Import and Export 'SPSS', 'Stata' and 'SAS' Files*, 2019, r package version 2.1.0, https://CRAN.R-project.org/package=haven.

[50] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2018, https://www.R-project.org/.

[51] Y. Xie, J. Allaire, and G. Grolemund, *R Markdown: The Definitive Guide*. Boca Raton, Florida: Chapman and Hall/CRC, 2018, iSBN 9781138359338, https://bookdown.org/yihui/rmarkdown.

[52] M. B. Miles and A. M. Huberman, *Qualitative data analysis: An expanded sourcebook*. Sage, 1994.

[53] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *biometrics*, pp. 159–174, 1977.

[54] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse." in *NDSS*, vol. 14, 2014, pp. 23–26, https://www.cs.ucy.ac.cy/courses/EPL682/papers/passwords-2.pdf.

[55] T. R. Tyler, *Why people cooperate: The role of social motivations*. Princeton University Press, 2013.

[56] L. A. Penner, J. F. Dovidio, J. A. Piliavin, and D. A. Schroeder, "Prosocial behavior: Multilevel perspectives," *Annu. Rev. Psychol.*, vol. 56, pp. 365–392, 2005.

[57] R. LaRose, N. J. Rifon, and R. Enbody, "Promoting personal responsibility for internet safety," *Communications of the ACM*, vol. 51, no. 3, pp. 71–76, 2008.

[58] B. J. Taylor, "Factorial surveys: Using vignettes to study professional judgement," *British Journal of Social Work*, vol. 36, no. 7, pp. 1187–1207, 2005.

[59] H. Aguinis and K. J. Bradley, "Best practice recommendations for designing and implementing experimental vignette methodology studies," *Organizational Research Methods*, vol. 17, no. 4, pp. 351–371, 2014.

[60] L. Sices, C. Feudtner, J. McLaughlin, D. Drotar, and M. Williams, "How do primary care physicians manage children with possible developmental delays? a national survey with an experimental design," *Pediatrics*, vol. 113, no. 2, pp. 274–282, 2004.

[61] M. Rungtusanatham, C. Wallin, and S. Eckerd, "The vignette in a scenario-based role-playing experiment," *Journal of Supply Chain Management*, vol. 47, no. 3, pp. 9–16, 2011.