# Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices

**Leave Authors Anonymous for Submission**

## ABSTRACT

Users struggle to adhere to expert-recommended security and privacy practices. While prior work has studied initial adoption of such practices, little is known about the subsequent implementation and abandonment. We conducted an online survey (n=902) examining the adoption and abandonment of 30 commonly recommended practices. Security practices were more widely adopted than privacy and identity theft protection practices. Manual and fully automatic practices were more widely adopted than practices requiring recurring user interaction. Participants' gender, education, technical background, and prior negative experience are correlated with their levels of adoption. Furthermore, practices were abandoned when they were perceived as low-value, inconvenient, or when users overrode them with subjective judgment. We discuss how security, privacy, and identity theft protection recommendations and tools can be better aligned with user needs.

## Author Keywords

User behavior; usable security and privacy; risk perception; adoption; abandonment.

## CCS Concepts

•**Human-centered computing → Empirical studies in HCI;** •**Security and privacy → Human and societal aspects of security and privacy;** *Privacy protections; Usability in security and privacy;*

## INTRODUCTION

There is a plethora of expert advice on how to stay safe online. Some advice addresses security risks (e.g., use antivirus software); some focuses on privacy (e.g., opt out of targeted ads); and some aims to mitigate risks of identity theft (e.g., place a credit freeze on one's credit reports). However, experts' recommendations are rarely taken by end-users [21,30,39,43,45].

While prior work has investigated why users adopt or reject expert-suggested practices, most studies focused solely on security practices [31,45,69,70]. Only a few examined privacy practices in specific contexts [1,33], but not holistically. Hardly any work has looked at the adoption of identity theft protection practices. Yet, privacy and identity theft risks are increasing in recent years, evidenced by a rising volume of privacy scandals, data breaches, and financial fraud [44,50,83] While advice in these areas is also increasing, little is known about how and why users adopt or reject privacy and identity protection practices, as well as if and how this may differ from user behavior in the security domain. Moreover, most prior work on advice adherence has focused on motivations and hurdles for initial advice adoption [31,45,74]. Reasons for incomplete, inconsistent implementation or abandonment of advice *after* initial adoption have not yet been examined systematically, despite potential risks generated from such behavior. For example, data breach victims who do not refreeze their credit reports after a loan application would still be at high risk of identity theft.

We provide a more holistic understanding of how and why people adopt, partially adopt, or abandon expert advice on security, privacy, and identity theft protection practices. We asked the following research questions: (RQ1) *Which* security, privacy, and identity theft protection practices are commonly adopted fully, adopted partially, and abandoned? (RQ2) *What* factors influence a practice's level of adoption? (RQ3) *Why* are certain practices partially adopted or abandoned?

We conducted an online survey with 902 U.S. adults on Prolific. Our survey queried 30 expert-recommended security, privacy and identity theft protection practices suggested by prior work [14,45,57,82]. Security practices were more widely adopted than privacy and identity theft protection practices. Both manual practices (i.e., the user needs to remember to adhere to the practice) and automated practices (i.e., little to no user effort is required after initial adoption) were more popular than practices requiring recurring user interaction (e.g., two-factor authentication). Participants' gender, education, technical background, and prior negative experience are correlated with their levels of adoption. Practices were abandoned when they were perceived as low-value, inconvenient, or when users overrode them with subjective judgment, such as believing they are tech-savvy enough to tell which sites are safe rather than obeying warnings from antivirus. Notably, participants sometimes made exceptions to practices that should be adopted consistently to be effective.

Based on our findings, we discuss how expert recommendations can be improved to better align with end-users' needs and encourage continuous and consistent adherence. We further identify opportunities for designing security, privacy and identity theft protection tools to promote such adherence, especially when recurring user interaction is required.

*CHI'20,* April 25–30, 2020, Honolulu, HI, USA

ISBN 978-1-4503-6708-0/20/04. . . $15.00

DOI: https://doi.org/10.1145/3313831.XXXXXXX

## RELATED WORK

We discuss prior research on expert-recommended best practices, how such recommendations are communicated to users, usability issues with existing tools, and people's mitigation behavior regarding security, privacy, and identity theft risks.

### Expert-recommended Practices for Online Safety

Experts and non-experts think and act differently when it comes to information security and privacy. Experts generally have more accurate mental models of complex systems and potential risks [10,15,47], but behave insecurely sometimes [26]. A variety of online safety advice for consumers is provided by corporate (e.g., [18,19,59]) and government organizations (e.g., [81,84]). Many organizations also mandate employee training prior to receiving network or computer access [28]. Yet substantial discrepancies exist between security practices taken by experts and non-experts, suggesting that the nature and delivery of expert advice could be improved [14,45]. Expert advice is often vague, unrealistic, or contradictory [71], and might not be economically rational, e.g., time spent checking URLs might exceed potential monetary loss from phishing attacks [40]. Improving the quality of expert advice requires keeping up with new and evolving attack vectors, empirically evaluating socioeconomic outcomes of advice, as well as a deep understanding of human behavior and effective risk communication [38,40,41,71].

### Security and Privacy Decision Making

Rational choice theory views humans as rational agents, and their decision to follow advice would occur only when benefits (e.g., protection from potential harm) exceed costs (e.g., time and effort to implement the advice) [4]. As such, one reason for rejecting security advice is *compliance budgets*, i.e., one can only devote limited time and resources to security behavior [12,62]. Both Fagan & Khan [31] and Ruoti et al. [74] found that users carefully weigh costs vs. benefits in choosing strategies to cope with security risks. Similarly, the *privacy calculus* theory explains users engage in online disclosure when perceived benefits (e.g., social validation, social capital gains) outweigh privacy loss [29,53,79,85,99].

Psychology-based theories also help explain security and privacy decisions. The *theory of planned behavior* [6] identifies the importance of beliefs, risk perception, and social influence. Objective knowledge can be overwritten by their inherent beliefs [93], such as “no matter what I do, I won't be 100% secure” [70,74], and “I've got nothing to lose” [102]. *Protection motivation theory* [72] suggests that threat perception and subjective assessment of coping mechanisms are crucial to forming the intention to act, and has been widely applied [9,20,46,77,98]. *Social cognitive theory* [11] further inspires a stream of research to highlight how security and privacy behaviors is influenced by observations of others, and advice received from trusted peers or media [21,23–25,70].

Behavioral economics research shows how security and privacy decisions are subject to bounded rationality, heuristics, and behavioral biases [2]. People's privacy preferences are uncertain, highly dependent on context, and malleable by government and corporate interests [3]. More sensitive information is disclosed when knowing others are doing so, and when stronger privacy controls are provided [5,13]. Similarly, security decisions are subject to overconfidence and optimism bias, such as in the wake of data breaches [102].

### User Demographics and Characteristics

Demographic factors, prior knowledge and experience also influence security and privacy behavior. Women tend to be more susceptible to phishing than men [37,76]. Younger people, despite heavier social media use and disclosure, engage more actively in privacy-protective behaviors [49,67]. People with lower incomes might struggle with identifying tools and strategies for protection, often due to limited access to the Internet and digital media [43,56,69]. More knowledge is generally correlated with higher intention to adopt safe practices and sensitivity to risks (e.g., phishing) [51,66]. Wash and Rader found, however, that more educated users held more sophisticated beliefs but took fewer precautions [94].

### Usability Issues with Existing Tools

Usability issues are a key contributor to partial adoption or rejection of online safety practices. For password managers, usability issues such as lacking support for biometric authentication and long setup time create barriers for adoption [7,8]. For two-factor authentication (2FA), users may feel its usability costs outweigh security improvements [17]. Tools that limit tracking and targeted advertising have numerous problems from confusing interfaces, broken links to insufficient feedback [36,54]. Persistent usability issues also exist in email encryption and key management tools [73,97]. Secure messaging apps like Signal or WhatsApp simplify key management, but adoption is still limited by fragmented user bases [1].

Compared to security and privacy tools, usability of identity theft protection services has received little attention. In Rosoff et al.'s scenario-based experiments, only 6% of participants reported paying for an identity theft protection service, but reasons for low adoption rates were unclear. Zou et al.'s qualitative study reveals usability issues with protective measures for dealing with the 2017 Equifax data breach, such as the inconvenience of remembering a PIN to lift and re-apply a credit freeze; these issues did not necessarily deter people from taking action, but still affected their experience [102].

#### *Abandonment of Security and Privacy Practices*

Usability issues not only create barriers for adoption but also sabotage user engagement afterwards, sometimes leading to abandonment. For instance, password managers were abandoned when they failed to store passwords accurately [64], while secure communication tools were abandoned due to low quality of service [1]. Users who updated software and had a bad experience were less inclined to update that software in the future [91]. However, aside from usability issues, we know little about what other reasons might be behind abandonment decisions. Through conducting this study, we contribute a deeper understanding of reasons behind partial adoption and abandonment (in general and for particular practices), as a step toward designing practices for long-term adherence.

## STUDY DESIGN

To provide a comparative assessment of adoption and abandonment of expert-recommended practices in different domains, we conducted an online survey with 902 participants in August 2019. We aimed to investigate which security, privacy, and identity theft protection practices are adopted, partially adopted, abandoned, considered, or rejected; what factors influence levels of adoption; and reasons for partial adoption or abandonment. We used survey to quantitatively analyze adoption and abandonment differences between individual practices and domains, draw inferences between user behavior and potential influential factors, as well as quantify reasons behind partial adoption and abandonment at scale. This study was approved by our university's Institutional Review Board (IRB).

### Taxonomy of Expert-Recommended Practices

We conducted an extensive literature search to determine what expert-recommended practices to be included (see Table 1). Prior work mostly associates online safety with security measures [45], but privacy and identity theft risks are increasing and closely linked. It is important to contrast and characterize user adherence to expert advice from these adjacent domains.

Our security-related practices (*n*=12) were primarily based on Ion et al.'s 2015 study on security advice: they surveyed >200 experts (5+ years work experience in computer security) about the top three pieces of online security advice they would give to non-tech-savvy users [45]. Most expert advice remained constant in Busse et al.'s 2019 replication study [14]. Because the number of unique advice is large (152 in total), we only took the 11 most-mentioned practices, which, according to the authors [71], are likely to be agreed on by most experts. For the advice of "be careful/think before you click," we followed the author's recommendation to instead ask about two more specific practices: "don't click links in email from unknown sender" and "check URL for expected site" [71].

For privacy and identity theft protection practices, due to challenges in finding a comparable research study systematically eliciting expert advice, we broadened our search to online articles, reports, and blog posts by experts from enterprises, government organizations, and NGOs. Our privacy-related practices (*n*=12) were primarily based on a census-representative 2015 Pew survey examining Americans' attitudes and behaviors about privacy [57]. This survey asked whether respondents had engaged in any of 13 everyday privacy-enhancing practices. We included all but two of those practices, for which consistent and frequent full adoption did not seem applicable or practical ("delete or edit something posted in the past" and "ask someone to remove something posted about you online"). We added the practice of opting out of facial recognition to unpack users' opinions and behaviors surrounding this emerging technology, given its substantial privacy implications [16, 78].

Our identity theft protection practices (*n*=6) came from the website of Federal Trade Commission's (FTC). We included practices clearly focused on identity theft protection (e.g., "place a credit freeze"). We excluded more general security or privacy practices (e.g., "don't overshare on social networking sites"), and practices that only apply to victimized individuals (e.g., identity recovery services), since most of our included practices focus on preemptive risk mitigation.

| **Practice** (Prefixed with **[Abbreviation, Nature]** of the Practice) |
|---|
| S1. **[2FA, Assisted]** Opt-in to 2FA for online accounts * |
| S2. **[Antivirus, Auto]** Use antivirus software * |
| S3. **[Attachment-clicking, Manual]** Beware of attachments sent by unknown people |
| S4. **[Automatic-update, Auto]** Keep automatic software updates turned on |
| S5. **[Check-URL, Manual]** Check the URL when visiting a website * |
| S6. **[HTTPS, Manual]** Check if the website visited uses HTTPS * |
| S7. **[Install-software, Manual]** Only install software from trusted sources |
| S8. **[Link-clicking, Manual]** Avoid clicking links sent by unknown people |
| S9. **[Password-manager, Assisted]** Use a password manager * |
| S10. **[Strong-password, Manual]** Use strong passwords for online accounts * |
| S11. **[Unique-password, Manual]** Use different passwords for each account |
| S12. **[Update-software, Manual]** Install OS and software updates immediately |
| P1. **[Anonymity-system, Assisted]** Use anonymity systems, such as Tor and VPN * |
| P2. **[Cookies-clean, Manual]** Clear web browser cookies and history * |
| P3. **[Cookies-disable, Auto]** Disable or turn off third-party browser cookies * |
| P4. **[Encryption, Assisted]** Encrypt phone calls, text messages or emails |
| P5. **[Extension, Auto]** Use browser extensions that block ads, scripts or tracking * |
| P6. **[Hide-info, Manual]** Refuse to provide info that is not essential to transactions |
| P7. **[Incognito, Assisted]** Use private browsing mode * |
| P8. **[Public-comp, Assisted]** Use a public computer to browse anonymously |
| P9. **[Real-name, Manual]** Avoid using websites that ask for real names |
| P10. **[Search-engine, Assisted]** Use search engines that do not track search history |
| P11. **[Temporary-credential, Manual]** Use fake identities for online activities |
| P12. **[Facial-recognition, Assisted]** Opt out of facial recognition when possible * |
| I1. **[Credit-freeze, Assisted]** Place a credit freeze * |
| I2. **[Credit-monitoring, Auto]** Use a credit monitoring service * |
| I3. **[Credit-report, Manual]** Obtain free copies of credit reports * |
| I4. **[Fraud-alert, Auto]** Place a fraud alert * |
| I5. **[Identity-monitoring, Auto]** Use an identity monitoring service * |
| I6. **[Statements, Manual]** Check for fraudulent charges on account statements |

*Further text explanation/screenshots were provided in survey to aid participants' understanding.

**Table 1. Security, privacy, and Id. theft protection practices included.**

#### *Defining the nature of required user effort*

In developing the taxonomy, we noticed that these practices vary in the level of required user involvement, which may explain differences in adoption and abandonment. *Manual* practices like *Link-clicking* require users to remember to adhere to the practice and then implement them on their own: success of the practice solely relies on the user's manual application and cognitive assessment. *Automatic* practices like *Extension* instead constitute the adoption of a particular tool or service that, after initial setup, runs in the background and provides automatic protection with minimal user involvement. *Assisted* practices, like *2FA*, also require the adoption of a tool or service, but users need to interact with them on a recurring basis for full protection.

### Survey Protocol

We conducted our study on Prolific, a crowdsourcing platform similar to Amazon's Mechanical Turk, but provides participants from a wider range of demographics who are not necessarily tech-savvy [60, 65]. We described the survey topic as "risk management when using the Internet" to avoid specific priming about security, privacy, or identity theft. Our survey targeted at people who reported U.S. as their nationality, were 18 years old or older, and had an approval rate of >90%. Participants were compensated $1.20 for work that generally took 5-10 minutes (mean = 9.68, median = 7.34), in line with Prolific's minimum hourly payment requirement.

| | |
|---|---|
| *Full adoption* | I am ALWAYS doing this. |
| *Partial adoption* | I am doing this but there are exceptions. Please describe it further: [text-entry box] |
| *Abandonment* | I am NOT doing this anymore, but I have done this before. Please describe it further: [text-entry box] |
| *Consideration* | I have NEVER done this before, but I EXPECT to do this in the near future. |
| *Rejection* | I have NEVER done this before, and I DO NOT EXPECT to do this in the near future. |
| *Unawareness* | I have NEVER heard of this/I do not understand. |
| *Other* | Other (please specify): [text-entry box] |

**Table 2. Response options relating to adoption for our survey questions.**

Upon accepting the task, participants were directed to our online survey. After agreeing to the consent form, each participant was shown 10 practices (4 security, 4 privacy, 2 identity theft) randomly selected from our list of 30 expert-recommended practices, displayed in randomized order. This enabled us to gain an average of $\sim$300 responses to each practice while minimizing respondent fatigue and ensuring data quality. To improve data quality, an attention check question was included at a random place among the 10 practices.

We used "Have you ever...?" as the consistent question format for all practices. We provide definitions of terms, tools, or services involved for practices that might not be immediately comprehensible to the general public, occasionally in addition to screenshots of relevant UI elements, to reduce chances of misconception and confusion (denoted by * in Table 1). For each practice, we asked participants if this is something they have *fully adopted*, *partially adopted*, *abandoned*, *considered*, *rejected*, *not understood*, or *other* (see Table 2). For four practices, we adjusted the response options to make them a better fit when a reference point is needed for participants to distinguish between full and partial adoption (e.g., defining "full adoption" as "making multiple requests throughout the year" for *Credit-report*), or when partial adoption does not really apply to the context (e.g., one either signs up for a credit monitoring service or not, but it is impossible to selectively apply the service), as echoed by participants in our pilot-tests.

After going through the 10 practices, participants were asked about prior negative experiences, namely someone accessing any of their online accounts without authorization, being a victim of a data breach, and being a victim of identity theft. People with such experience might be more cautious and more prone to adopting protective measures. The survey concluded with demographic questions about age, gender, income, education, employment, and background in computer science (CS)/information technology (IT) as well as security/privacy. All survey questions were required, and a "Prefer not to answer" choice was offered for potentially sensitive topics. The full survey is included in our supplemental materials.

## Data Analysis

After removing 17 participants who failed the attention check question, we received 902 complete survey responses. Data preparation and analysis steps are described below.

### Qualitative data analysis

Participants provided 1,728 open-ended responses in total. Among these, 69% were explanations for partial adoption, 25% for abandonment, and 6% for other. We developed a codebook to analyze reasons for partial adoption and abandonment. The first author went through all responses and developed codes using inductive coding [52]. Two co-authors then independently analyzed 150 (8.7%) randomly sampled responses, reconciling codes and revising the codebook iteratively until reaching a high inter-coder reliability (Cohen's $\kappa$=.82). The two co-authors then split the dataset and coded all responses. Our final codebook is included in the supplemental materials.

### Recode close-ended responses for practices

In going through participants' open-ended responses about partial adoption and abandonment, we realized some responses clearly pointed at other options in the list. For instance, one participant selected "other" for (*Fraud-alert*) and said "I have heard of this, but I have never done it before. It's possible I could do it in the future," which was a clear match for *consideration*. Two authors recoded these responses to minimize report biases and inconsistencies in the data. In total, 171 responses were recoded, of which 75 were originally *abandonment*, 71 were *other*, and 25 were *partial adoption*.

### Statistical analysis

Using the recoded dataset, we calculated descriptive statistics for rates of full adoption, partial adoption, abandonment, etc., for each practice. Motivated by prior work suggesting the influence of tool usability issues and user characteristics on user behavior, we constructed a series of mixed-effect regression models. For fixed-effect factors, we included characteristics related to the user (demographics, technical background, prior negative experience) and the practice (domain, nature of protection), all treated as categorical variables. We further included random effects resulting from differences between individual participants and practices when fixed-effect factors are under control. The intraclass correlation coefficient (ICC) for all models are below .20, indicating weak similarity between participants who responded to the same practice and between practices that were answered by the same participants.

To understand what factors influence users' levels of adoption at the moment of taking the survey, we performed linear regressions on an adjusted scale of response options, from 0 as no adoption (combining *abandonment*, *consideration*, and *rejection*), 1 as *partial adoption*, and 2 as *full adoption*, excluding rare cases of *unawareness* or *other*. The regression coefficient of each categorical predictor shows to what extent the predictor, compared to the baseline, brings the outcome up or down on this scale. We ran the model first on the whole dataset, before adding interaction terms between practice domain and other predictors to see how effects of these predictors vary across security, privacy, and identity theft domains. To understand what factors influence a practice being abandoned instead of adopted, we further tried running logistic regressions on a binary variable where "yes" means *abandonment* was selected, and "no" means *partial adoption* or *full adoption* was selected, excluding other response options. However, due to the small number of abandonment cases in our dataset (534 "yes", 5325 "no") the model failed to converge, as is to be expected. Therefore, we refrain from making statements about which variables are correlated with abandonment.

| Metric | Sample | Census |
|---|---|---|
| Women, Men, Non-binary | 50.0%, 48.0%, 1.8% | 51.0%, 49.0%, N/A |
| High school, Some college | 10.9%, 25.9% | 28.6%, 19.0% |
| Trade/vocational, Associate | 2.9%, 10.4% | 4.1%, 5.5% |
| Bachelor's, Master's | 34.4%, 11.7% | 20.6%, 8.5% |
| Doctoral, Professional | 1.3%, 1.3% | 1.8%, 1.3% |
| 18-24, 25-34 years | 22.3%, 29.6% | 9.3%, 14.0% |
| 35-44, 45-54 years | 22.6%, 13.6% | 12.6%, 12.7% |
| 55-64, 65-74 years | 7.9%, 3.6% | 12.9%, 9.3% |
| 75 years or older | <1% | 6.7% |
| <$20k | 16.5% | [10.2%, 19.1%] |
| $20k-$35k | 17.2% | [8.8%, 17.7%] |
| $35k-$50k, $50k-$75k | 15.3%, 21.6% | 12.0%, 17.2% |
| $75k-$100k, >$100k | 12.2%, 14.5% | 12.5%, 30.4% |

**Table 3. Gender, education, age and income demographics of survey participants. Census statistics from [86–89].**

## Limitations

While the scope of our investigation exceeds most prior work, there might be other practices related to security, privacy, identity theft protection or additional areas related to safety, such as harassment and cyberbullying [68]. Most of our practices are applicable to the general public and focus on the online context, but future research can go beyond this.

As with any survey, participants in our study may over-report their behavior due to social desirability bias [32]. This effect may be particularly salient for *full adoption* when participants think they are always implementing a practice while forgetting about certain exceptions. To mitigate this, we provided instructions to encourage honest answers and guarantee responses would be anonymized. The main goal of our survey is not to provide empirical field measurements about actual behavior regarding each practice, but rather to understand, in the participants' own opinion, what practices they think they fully adopt and what others are deliberately adopted only in certain situations or fully abandoned.

Another point concerning consistency is the adjustment we made to certain practices, e.g., removing partial adoption as one of the response options for *Credit-monitoring*, *Identity-monitoring*, *Credit-freeze*, and *Fraud-alert*. While this makes the results of partial adoption for identity theft protection practices less comparable to those for security or privacy protection, we considered this an important measure to increase clarity and reduce confusion for the survey, as partial adoption does not technically apply to these practices.

## RESULTS

Below we describe our participant sample, highlight some of the most adopted and abandoned practices, and present factors and reasons behind adoption and abandonment behavior.

### Participant Demographics and Profile

Table 3 compares our sample to U.S. demographics. Our participants are evenly distributed between men and women, but are more educated and skew younger. Their income levels cover a wide range, but fewer participants live in a household with more than $100k annual income. Regarding educational background or work experience related to CS/IT and security/privacy, 66.6% had a background in neither domain, 11.6% only in CS/IT, 8.0% only in security/privacy, and 11.0% in both. Furthermore, 67.0% have been victims of a data breach; 35.0% have been victims of unauthorized account access; and 11.3% have been victims of identity theft.

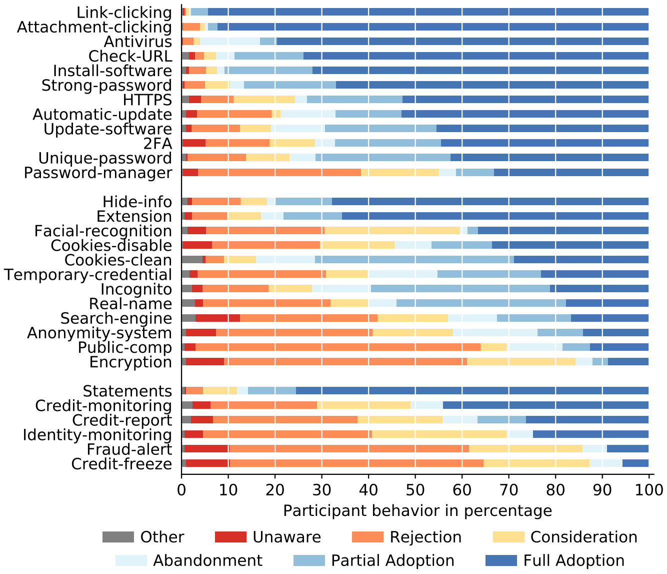

**Figure 1. Distribution of response options for each practice.**

### RQ1: Commonly Adopted and Abandoned Practices

Figure 1 shows the percentage distribution of response options for each practice. Overall, security practices had the highest full adoption rates, while partial adoption and abandonment were concentrated in privacy practices. Most identity theft mitigation practices had never been adopted, and a fair amount of participants reported they would not consider them either.

#### *High adherence to security practices*

Of 10 practices with the highest full adoption rate, 7 are security practices, with the top 2 reflecting the importance of cautious clicking behavior (94.6% for links, 92.6% for attachments). Two privacy practices were also fully adopted at high rates, namely *Hide-info* (69.0%) and *Extension* (68.0%). *Statements* was the only identity theft protection practice that was fully adopted by over half of participants (76.2%). Except for *Antivirus* and *Extension*, these commonly fully adopted practices are manual, situated in people's everyday interactions with computers, and not overly technical.

#### *Partial adoption exists for both security and privacy practices*

As we did not provide partial adoption as a response option for 4 of 6 identity theft protection practices, we only report partial adoption results for security and privacy practices. Overall, practices with high partial adoption rates were evenly split between the security and privacy domains, with the top three all being about privacy risk management (49.7% *Cookies-clean*, 39.9% *Incognito*, 39.1% *Real-name*). Consistent with prior work [55,63,80], a substantial fraction of participants did not fully follow expert-recommended password management practices (29.4% *Unique-password*, 21.4% *Strong-password*).

#### *Abandonment mostly occurred for privacy practices*

Abandonment rates were below 20% for all practices and less common than full or partial adoption overall. 7 of the 10 practices with the highest abandonment rates were privacy practices, with *Anonymity-system* being the most common (16.8%). *Automatic-update* (13.3%) and *Antivirus* (11.0%) were the most abandoned security practices, while 7.2% had abandoned *Credit-monitoring*. Some commonly abandoned practices appear rational, since they seem more realistic for one-time use rather than long-term implementation (e.g., *Public-comp*). Other abandoned practices do require consistent and periodic implementation for effective protection (e.g., *Cookies-clean*).

### *Low adoption/acceptance of practices against identity theft*

Among practices that had not been adopted as yet by most participants, many pertain to identity theft risk mitigation. The top practice that was considered for implementation in the near future is *Facial-recognition* (29.2%), followed by *Identity-monitoring* (28.9%), *Fraud-alert* (24.6%), and *Credit-freeze* (23.1%). Most of these top considered practices require adopting new tools or services, either automated tools that protect in the background (e.g., credit/identity monitoring) or tools that assist users and require recurring user interaction (e.g., password managers). Nonetheless, automated practices like *Credit-freeze* and *Fraud-alert* are also among the top rejected practices (54.5% and 51.2%, respectively). This is concerning given that 66% of our participants reported being data breach victims, and that these practices are among the most commonly recommended measures in data breach notifications [101].

## RQ2: Factors Affecting Levels of Adoption

We use mixed-effect linear regression models to confirm RQ1 findings that different levels of adoption can be predicted based on the practice's domain and its type of user interaction. We further use these models to investigate effects from user characteristics and found significant effects from demographics, technical background, and prior negative experiences. Next, we describe and interpret these significant factors.

### *Levels of adoption: security $>$ privacy $\geq$ identity theft*

Confirming the descriptive analysis, our regression model shows that security adoption levels were significantly higher than for privacy practices ($b$=.43, $p$<.01) or identity theft protection practices ($b$=.62, $p$<.001). While privacy practices exhibit higher levels of adoption than identity theft protection practices, the difference is not significant ($b$=.20, $p$=.21).

### *Practices requiring recurring interaction less adopted*

We were particularly interested in whether a practice's degree of user interaction (manual, assisted, automated) affects adoption. We expected that practices relying on manual effort to be least often adopted, due to higher cognitive demand leading to errors or inconsistent behavior. Our results show the opposite: assisted practices, which require recurring user interaction, were adopted the least, with manual ($b$=.64, $p$<.001) and automated ($b$=.53, $p$<.01) practices exhibiting significantly higher levels of adoption. Significant differences between practices offering manual versus assisted protection persist within security ($b$=.58, $p$<.05), privacy ($b$=.51, $p$<.05), and identity protection practices ($b$=1.02, $p$<.001).

### *Gender and age differences in levels of adoption*

We further identify significant effects for certain user characteristics. We find significantly higher levels of practice adoption for men compared to women overall ($b$=.08, $p$<.001), and within security practices ($b$=.11, $p$<.001) and privacy practices ($b$=.11, $p$<.01) in particular. This confirms prior work showing similar gender differences for phishing susceptibility [37, 76] and extends it to a wider range of practices.

We mapped age to the following categories: 18-34, 35-54, and 55+. We find significant age differences for security and privacy, but not overall. Middle-aged participants (35-54 years old) exhibited higher levels of security practice adoption than younger participants ($b$=.07, $p$<.05). This aligns with the findings in [58] that people belonging to older age brackets demonstrate higher information security awareness. The opposite trend emerged for privacy practices, for which younger participants had significantly higher levels of adoption than middle-aged ($b$=.14, $p$<.001) and older participants ($b$=.23, $p$<.001). This extends the finding in [49], that young adults are more likely to engage in privacy-protective behaviors on Facebook, to other privacy practices.

### *Higher adoption among low-income participants*

We mapped participants' annual household income to the following categories: <$50k, $50-100k, and >$100k. The overall trend is that participants with lower incomes exhibit higher levels of practice adoption, though no significant differences were found between any two groups. When looking at individual domains, those earning <$50k had significantly higher levels of privacy practice adoption than those earning >$100k ($b$=.13, $p$<.01). Though seemingly counter-intuitive, as higher-income people should have stronger motivation and more resources to protect their privacy and assets, it confirms findings that people with lower incomes have heightened informational and physical privacy and security concerns [56], which might translate into the adoption of protective practices that are accessible and affordable to them.

### *More education contributed to higher adoption*

We mapped participants' educational background to the following categories: less than Bachelor's degree, Bachelor's degree or equivalent, and Graduate degree. More educated participants exhibited higher levels of practice adoption overall. In particular, participants with a Bachelor's degree had significantly higher adoption than those without ($b$=.05, $p$<.05). This holds true for identity protection practices ($b$=.24, $p$<.001), but not for security or privacy. This differs from Wash and Rader's finding that more educated people tend to take fewer security precautions [93], particularly with regard to mitigating identity theft risks.

11% of participants reported having a background both in CS/IT and security/privacy, and could therefore be considered experts. Their levels of practice adoption were significantly higher than those of the 67% who had no background in either field ($b$=.15, $p$<.001). Interestingly, this difference between experts and non-experts holds true when considering CS/IT only ($b$=.09, $p$<.01), but not for participants who only reported a background in security/privacy but not CS/IT. This suggests that technology experience and expertise might have a larger influence on practice adoption than security/privacy knowledge alone, which, as our participants reported in open-

| Partial Adoption | Count | Abandonment | Count |
|---|---|---|---|
| site-specific | 179 | not-needed | 68 |
| only-sensitive | 129 | because-of-risk | 50 |
| impractical | 124 | impractical | 41 |
| own-judgment-sufficient | 111 | usage-interference | 23 |
| because-of-risk | 95 | own-judgment-sufficient | 21 |
| usage-interference | 80 | using-substitute | 21 |
| only-finance | 74 | platform-specific | 17 |

**Table 4. Top coded reasons for partial adoption and abandonment.**

ended responses, was mostly based on university courses or employer-mandated trainings.

### *Experiencing security incidents contributes to high adoption*

Experiences with security incidents significantly affect practice adoption in general. Participants who had been victims of data breaches ($b$=.05, $p$<.05) or identity theft ($b$=.16, $p$<.001) reported significantly higher levels of adoption. By contrast, unauthorized access to online accounts had no significant effect. In particular, both data breach ($b$=.34, $p$<.001) and identity theft experience ($b$=.33, $p$<.001) contribute to higher levels of adoption of identity protection practices. Identity theft experience is correlated with higher levels of adoption in each of the individual domains ($b$=.11, $p$<.05 for security; $b$=.14, $p$<.01 for privacy; $b$=.33, $p$<.001 for identity), suggesting it is a robust trigger for pro-safety behaviors.

## RQ3: Reasons for Partial Adoption and Abandonment

Participants were asked to provide explanations when indicating partial adoption or abandonment of a practice. The most prevalent reasons for each are shown in Table 4. Tables 5 to 7 provide the top three partial adoption and abandonment reasons for individual practices. To provide more informative results, we do not report reasons coded as *unclear* (i.e., unintelligible or irrelevant) or reasons that only describe adoption *frequency* (i.e., "I do this sometimes").

### *Reasons for partial adoption*

As shown in Table 4, 179 participants (15%) who selected "partial adoption" described selectively using the practice for specific sites, apps, accounts, or software (coded as *site-specific*). This was the most common reason for privacy practices like *Real-name* (57 participants, see Table 1 for definitions of all practices) and *Temporary-credential* (31). Unfortunately, most participants did not specify where they applied the practice selectively. For those who did, 129 (27%) did so for sensitive sites (*only-sensitive*), 74 (6%) for finance-related sites (*only-finance*), 41 (3%) only for suspicious or odd sites (*only-suspicious*), and 16 (1%) for social-media and gaming services (*only-entertainment*). For practices adopted when visiting sensitive sites, 47 participants reported that they used *Incognito* browsing to interact with sensitive websites (e.g., adult sites, dark web), in line with prior work [35]. Other privacy practices were also adopted for this reason, though less frequently, such as *Anonymity-systems* (8) or *Search-engine* (8). Some mentioned they would take extra precautions when sensitive information is finance-related, such as using *2FA* (20), checking for *HTTPS* (15), and using *Unique-passwords* (10).

Another prominent reason for partial adoption cited by 124 participants (10%) was the practice being inconvenient or unusable, resulting in difficulty for consistent adherence (*impracticality*). The inconvenience of many security practices was highlighted, including *2FA* ("very annoying"), *Update-software* ("if I am in the middle of something I will not [do it]"), and *Unique-password* ("it's hard to keep track"). Inconvenience extended to privacy practices, including *Cookies-clean* (12, e.g., "it kills all my passwords") and *Incognito* (11, e.g., " I like to be able to have a list of the places I visited if I need to go back"). A small fraction of participants mentioned the practice was simply too hard to follow consistently. They referred to "rare occasions where I slip up" despite best intentions. Such failures might be more common in real life than reflected in our self-reports due to social-desirability bias and difficulties in recognizing when mistakes have been made.

111 participants (9%) rely on their own judgment to determine when it is safe to depart from best practices (*own-judgment-sufficient*). For security practices, this usually means installing software from suspicious sources (20), not always enabling automatic updates (10), and opening attachments from unknown people (5). For example, in talking about *Attachment-clicking*, one participant said: "I don't click on obvious spam e-mails, but I am willing to open e-mails that seem legitimate even if I don't know the senders," which is concerning given that even trained individuals routinely fall for phishing emails [76]. Similar trends manifested for privacy practices, with 9 participants disregarding the *Hide-Info* practice when they trusted the service, e.g., "I do play this by ear depending on the website and my familiarity with it."

95 participants (8%) reported adopting practices only when motivated by a perceived risk (*because-of-risk*), particularly for identity protection practices, such as *Statements* (21) and *Credit-report* (6). The at-risk feeling also motivates use of *Strong-password* (11) and *Anonymity-system* (9). For identity theft protection practices, adoption normally occurred after a data breach, a lost credit card, or when anomalous activity appears on a bank or credit statement. Security risks revolved mostly around account hacking due to weak passwords. The most common privacy practice in this category was using a VPN when "connected to untrustworthy or unsafe networks."

Finally, 80 participants (7%) reported struggling with practices that broke existing functionality or disrupted normal use of the device or service (*usage-interference*), such as *Update-software* (23), *Extension* (17), and *Cookies-disable* (12). Users selectively abandoned updates when buggy updates had "broken drivers, programs, or the OS itself" (in line with [91]), whitelisted sites on which browser extensions "blocked things I didn't want it to block," and allowed cookies when needed for the functionality of a site.

### *Reasons for abandonment*

Top reasons for abandonment are summarized in Table 4. We primarily discuss cases in which abandonment reasons differ from partial adoption justifications.

The most common reason for abandonment, cited by 68 participants (20%) was that the practice was not needed anymore (*not-needed*). These users generally did not see sufficient value in the practice to continue its use, e.g., "I decided it was useless." While this reason was expressed across domains,

| Security Practice | *n* | Top Three Reasons for Partial Adoption | *n* | Top Three Reasons for Abandonment |
|---|---|---|---|---|
| Update-software | 95 | usage-interference (23), impractical (22), own-judgment-sufficient (11) | 9 | usage-interference (4), impractical (3), performance-issues (2) |
| Unique-password | 93 | impractical (25), site-specific (17), because-of-risk (14) | 2 | because-of-risk (1), forgetting (1) |
| 2FA | 68 | only-finance (20), only-sensitive (16), impractical (6) | 10 | impractical (6), distrust-service (1), not-needed (1) |
| HTTPS | 62 | only-sensitive (23), only-finance (15), forgetting (11) | 3 | not-needed (1), practice-by-default (1), using-substitute (1) |
| Strong-password | 59 | because-of-risk (11), impractical (10), only-finance (10) | 3 | not-needed (1), only-required (1), site-specific (1) |
| Install-software | 51 | own-judgment-sufficient (20), usage-interference (13), impractical (10) | 4 | impractical (2), own-judgment-sufficient (1), using-substitute (1) |
| Check-URL | 44 | using-substitute (11), forgetting (8), only-suspicious (8) | 6 | only-suspicious (3), because-of-risk (1), unrelated-reason (1) |
| Automatic-update | 37 | own-judgment-sufficient (10), platform-specific (8), site-specific (5) | 37 | own-judgment-sufficient (13), impractical (9), usage-interference (8) |
| Password-manager | 24 | site-specific (7), using-substitute (6), impractical (3) | 7 | platform-specific (3), distrust-service (1), impractical (1) |
| Antivirus | 12 | platform-specific (3), because-of-risk (2), only-required (2) | 30 | platform-specific (12), own-judgment-sufficient (4), distrust-service (3) |
| Link-clicking | 8 | only-suspicious (2), own-judgment-sufficient (2), using-substitute (2) | 1 | impractical |
| Attachm.-clicking | 6 | own-judgment-sufficient (5), impractical (1) | 1 | impractical |

**Table 5. Participants' most frequent reasons for incomplete adoption and abandonment of security practices.**

| Priv. Practice | *n* | Top Three Reasons for Partial Adoption | *n* | Top Three Reasons for Abandonment |
|---|---|---|---|---|
| Real-name | 116 | site-specific (57), own-judgment-sufficient (30), using-substitute (14) | 6 | not-needed (2), own-judgment-sufficient (1), unapplicable (1) |
| Incognito | 110 | only-sensitive (47), impractical (11), site-specific (11) | 20 | not-needed (5), using-substitute (4), account-or-device-sharing (2) |
| Cookies-clean | 86 | unrelated-reason (36), forgetting (14), impractical (12) | 13 | impractical (4), forgetting (2), not-needed (2) |
| Temp.-credential | 71 | site-specific (31), because-of-risk (11), only-suspicious (11) | 22 | because-of-risk (9), only-suspicious (4), not-needed (3) |
| Search-engine | 45 | only-sensitive (8), own-judgment-sufficient (7), because-of-risk (5) | 14 | not-needed (9), impractical (2), unrelated-reason (2) |
| Cookies-disable | 37 | usage-interference (12), site-specific (6), own-judgment-sufficient (5) | 12 | using-substitute (3), impractical (2), unrelated-reason (2) |
| Extension | 32 | usage-interference (17), site-specific (6), own-judgment-sufficient (5) | 11 | usage-interference (5), not-needed (4), performance-issues (1) |
| Anon.-system | 30 | because-of-risk (9), only-sensitive (8), usage-interference (4) | 42 | not-needed (13), only-blocking (10), only-sensitive (4) |
| Hide-info | 27 | own-judgment-sufficient (9), site-specific (6), impractical (4) | 1 | site-specific |
| Public-comp | 17 | not-needed (4), distrust-service (3), using-substitute (3) | 18 | not-needed (10), unrelated-reason (4), because-of-risk (2) |
| Encryption | 10 | only-sensitive (4), as-needed (2), platform-specific (2) | 7 | because-of-risk (2), only-required (2), when-offered-free (2) |
| Facial-recog. | 7 | only-entertainment (3), platform-specific (2), forgetting (1) | 1 | unapplicable |

**Table 6. Participants' most frequent reasons for incomplete adoption and abandonment of privacy practices.**

it was salient for privacy practices particularly, with 5 of 10 privacy practices abandoned most likely because their value was not recognized (see Table 6). 4 of the 5 practices pertained to browsing activities, with the following comments on *Incognito* being representative: "I have used it but don't find it all that helpful," and "I did it once, just to see how it worked, but found it awkward."

In 50 abandonment cases (14%) participants abandoned a practice after perceiving that risk levels had diminished (*because-of-risk*). This justification was the dominant reason for abandoning *Fraud-alert* and *Credit-freeze*, which were commonly adopted after a fraud or lost/stolen credit card incident and dropped soon afterwards. Similarly, 11 participants had adopted *Temporary-credential* when engaging with risky services, but abandoned it either because of its negative repercussions, (e.g., "when I made friends it was embarrassing to have to admit I lied about my name") or because their online social interaction habits changed (e.g., "I've done this before when I used to have fights with people on the internet, but I don't anymore").

Participants abandoned practices due to their *impracticality* in 41 instances (12%), providing complaints similar to those for partial adoption. 23 participants (7%) reported abandoning practices when they caused *usage-interference*, mostly citing the same set of practices that were partially adopted by others.

In 21 abandonment cases (6%), participants abandoned a practice in favor of relying on their own judgment (*own-judgment-sufficient*). This was most prominent for abandoning *Automatic-update* (10) to regain control over the "what and when" of software updates, e.g., "I used to have them on because that was the default setting. Now I am more mindful of what software updates I actually want."

Another 21 participants (6%) abandoned a practice after adopting a service that served a similar purpose (*using-substitute*). This reason was mentioned for practices across all three domains. We noted a trend of switching to tools that offer automated protection from relying on manual effort, as in the case of *Cookies-disable* (3), e.g., "I run programs to clear my cookies frequently." Most participants made sensible decisions when supplanting recommended practices with their own solutions. For instance, "If I visit a website I have bookmarked I don't check [the URL] as I already verified it before I bookmarked the site." *Password-manager* is the rare case where substitutes appeared to be less effective, e.g., "I use a password manager, but only to store passwords I create. I do not use the password generator. I usually create long, difficult passwords that are more memorable to me than what a generator produces." However, prior research suggests that users' self-generated passwords are typically weaker than random passwords generated by password managers [63].

## DISCUSSION

Our findings provide insights on how well security, privacy, and identity theft protection practices are adopted, and in particular why certain practices are only partially adopted or abandoned. We discuss how expert recommendations, as well as tools and services for security, privacy, and identity theft protection could be improved.

### Implications for Expert Recommendations

Users struggle to adhere to experts' online safety advice [21, 43] and expert advice is often vague, inactionable, and contra-

| Id. Prot. Practice | *n* | Top Three Reasons for Partial Adoption | *n* | Top Three Reasons for Abandonment |
|---|---|---|---|---|
| Statements | 28 | because-of-risk (21), using-substitute (4), not-needed (2) | 5 | unapplicable (3), not-needed (2) |
| Credit-report | 14 | because-of-risk (6), unrelated-reason (5), when-offered-free (2) | 12 | not-needed (6), using-substitute (2), because-of-risk (1) |
| Id.-monitoring | | N/A | 10 | when-offered-free (3), because-of-risk (2), using-substitute (2) |
| Credit-monitoring | | N/A | 12 | not-needed (4), when-offered-free (4), because-of-risk (1) |
| Fraud-alert | | N/A | 14 | because-of-risk (11), impractical (1), unapplicable (1) |
| Credit-freeze | | N/A | 15 | because-of-risk (14), usage-interference (1) |

**Table 7. Participants' most frequent reasons for incomplete adoption and abandonment of identity protection practices.**

dictory [41, 71]. Our findings suggest ways to develop better expert advice and effectively convey it to consumers.

### *Bridge the gap between security and other safety practices*

While security practices exhibited relatively high adoption rates in our survey, most privacy practices were often either used selectively or abandoned, and many identity theft protection practices were not even considered. This finding is concerning given that practices from different domains often complement each other. For example, phishing is a common attack vector for identity theft [61]. Manual security practices (e.g, *Link-clicking*) are prone to cognitive errors and inconsistent application, in which case assisted security (e.g., *2FA*) and identity theft protection practices (e.g., *Credit-freeze*, *Fraud-alert*), can help prevent account compromise and identity theft; identity monitoring services can further facilitate mitigation and recovery in cases of compromise. Thus, adoption of multiple practices across domains can create additional security layers and synergistic effects.

Security is usually conceived as something related to passwords, antivirus, or cautious interactions with websites and emails [14, 45]. Thus, security advice and education need to also cover related privacy and identity protection practices to help people achieve a more holistic online safety posture. Rather than overburdening users with too much advice, experts should identify most effective and actionable recommendations from each area, and articulate how they complement each other and together create safety gains beyond those from adopting a single practice.

### *Leverage at-risk situations for communicating advice*

Prior work has identified triggers for adopting security and privacy practices [21]. Our findings show that experiencing security incidents, especially identity theft, drives adoption of protective measures across all three domains. As such, opportunities to convey advice more effectively might exist in post-incident guidance, when people are highly motivated to resolve the situation and mitigate future risks. Required security and privacy notices such as data breach notifications could be leveraged accordingly [101]. Similar to phishing training materials [92], for people who are not direct victims of security incidents, vivid and detailed stories recounting the negative experiences of living through an incident (e.g., on being an identity theft victim [96]) might be more effective than merely listing factual harms. Such stories should further be combined with actionable preventative advice.

Nevertheless, practice adoption triggered by negative experiences might not be long-term. Our participants reported taking certain practices only in high-risk situations, and abandoned the practice soon after the perceived risk decreased. Such abandonment of risk-triggered behaviors should be assessed critically. Some practices might not be relevant anymore due to changes in circumstances (e.g., not needing incognito mode anymore when no longer sharing a device). Yet interventions are needed when perceptions of decreased risk are misaligned with objective risks. For instance, participants abandoned *Credit-freeze* and *Fraud-alert* soon after data breaches, even though the objective identity theft risks may not change over time once sensitive information has been exposed. Expert advice to users needs to more clearly communicate risk persistence, i.e., what practices can be used selectively (and in which situations), and what other practices require consistent long-term adoption to be effective.

### *Tailor advice to audience characteristics*

Prior research suggests a "digital divide" in security and privacy: people with lower education and socioeconomic status may have access to fewer resources, exposing them to further vulnerability [48, 69]. Our findings are more nuanced. More technology knowledge is linked with higher levels of practice adoption (interestingly, security/privacy expertise alone had no effect). However, lower income also contributes to higher adoption, especially for privacy practices, possibly because people with lower incomes might be more acutely aware of digital privacy harms [56]. Notably, most investigated privacy practices are free or have free options (e.g., *Anonymity-system*). These results confirm the need for expert advice to be tailored to specific audiences to be effective [56]. For instance, the use of personas [27] and scenarios reflecting different audiences and their needs could help users identify solutions most suitable to them, yet need to be crafted carefully to be inclusive.

## Implications for Design

Building on prior work, our study shows that usability issues widely exist across security, privacy, and identity theft protection practices, and function as a key contributor to partial adoption and abandonment. We identify which practices most require usability improvements or the design of more usable alternatives. While usability research has largely focused on security practices, usability of privacy and identity protection practices calls for more attention. Additionally, tools and services that demand consistent user interactions were adopted the least, indicating the need for improvement.

### *Usability issues prevent full adoption across practices*

Usability issues are a key contributor to partial adoption and abandonment across practices instead of specific ones, e.g, *Update-software* [91], *Password-manager* [64] and *Unique-password* [63]. Practices being difficult or inconvenient to implement was a main reason for partial adoption and abandonment, even when users saw value in the practice. In line with prior work [91, 95, 100], updates in particular can be inconvenient and even severely disruptive. While prior work has focused largely on improving usability of assisted security practices (e.g., *2FA* [22]), more usability research needs to focus on commonly abandoned or rejected privacy and identity protection practices in order to lower their barriers for adoption. Browsing-related privacy practices in particular have significant usability issues and deserve more attention. For instance, *Cookies-clean* was considered impractical as it also removes desired cookies (e.g., session and login cookies). Similar to purpose-oriented cookie consent banners [90], browsers and web standards could support cookie management controls that distinguish different types of cookies to let users set more meaningful preferences.

*Improve support for practices requiring recurring interactions* Concerningly, practices requiring recurring interactions have significantly lower adoption rates than both manual and automated practices. While the included manual practices are instructive rules of thumb (e.g., "don't click unknown links"), they are prone to slip-ups and are easily overruled by users' judgement as our results show. Conversely, most assisted practices (e.g., *Anonymity-system*, *Password-manager*) generally require some level of expertise for initial setup, which may scare non-tech-savvy users away [8, 64], or have known usability issues that significantly impact user experience [73, 75].

For tool-based practices (e.g., *Password-manager*), their features and functionality need to be better communicated to prospective users to dispel identified misconceptions. Additionally, required user effort should be reduced where possible. For instance, most participants who adopted *Password-manager* chose those built into their browsers due to direct integration into the browsing experience, whereas dedicated password managers often require extra steps to retrieve passwords. Even eliminating a few clicks can make a big difference as users' compliance budgets are extremely limited [41]. Lastly, small tweaks to mechanisms can have diminishing returns compared to paradigm changes. For instance, biometric authentication, despite its flaws and weaknesses, can be used in combination with password managers to ease adoption and usability of multiple practices at once [34, 42]. Furthermore, recurring interactions should be designed to convey the value of associated protection so they are not just perceived as a nuisance.

## CONCLUSION

Our survey (n=902) examined the adoption and abandonment of 30 common expert-recommended online safety practices. We identify discrepancies and respective reasons in levels of adoption among security, privacy, and identity theft protection practices. We contribute novel insight on the impact of involved user interactions on practice adoption, with practices requiring recurring interactions being least preferred. We further show the influence of gender, education, background, and prior negative experience on practice adoption, and how it varies across domains. We provide recommendations for improving expert advice and usability of tools and services to better align with users' needs and foster long-term adoption.

## REFERENCES

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 137–153.

[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. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 44.

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[4] Alessandro Acquisti and Jens Grossklags. 2003. Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS*, Vol. 3. 1–27.

[5] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2012. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research* 49, 2 (2012), 160–174.

[6] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[7] Nora Alkaldi and Karen Renaud. 2016. Why do people adopt, or reject, smartphone password managers?. In *1st European Workshop on Usable Security. Internet Society*.

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

[9] Catherine L Anderson and Ritu Agarwal. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly* 34, 3 (2010), 613–643.

[10] Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. In *International Conference on Financial Cryptography and Data Security*. Springer, 367–377.

[11] Albert Bandura. 1999. Social cognitive theory: An agentic perspective. *Asian journal of social psychology* 2, 1 (1999), 21–41.

[12] Adam Beautement, M Angela Sasse, and Mike Wonham. 2009. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 47–58.

[13] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347.

[14] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[15] L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and society magazine* 28, 3 (2009), 37–46.

[16] Angela Chen. 2019. Most Americans are fine with cops using facial recognition on them. `https://www.technologyreview.com/f/614267/facial-recognition-police-law-enforcement-surveillance-privacy-pew-research-survey/`. (2019). Last accessed on: 09.15.2019.

[17] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 456.

[18] Mozilla Corporation. 2019a. Security tips to protect yourself from hackers. `https://monitor.firefox.com/security-tips`. (2019). Last accessed on: 08.31.2019.

[19] Symantec Corporation. 2019b. Symantec Support: How can we help you. `https://support.symantec.com/us/en.html`. (2019). Last accessed on: 08.31.2019.

[20] Robert E Crossler. 2010. Protection motivation theory: Understanding determinants to backing up personal data. In *43rd Hawaii International Conference on System Sciences*. IEEE, 1–10.

[21] Sauvik Das, Laura Dabbish, and Jason Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 97–115.

[22] Sanchari Das, Andrew Dingman, and L Jean Camp. 2018. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *Proceedings of the International Conference on Financial Cryptography and Data Security*.

[23] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *Tenth Symposium On Usable Privacy and Security (SOUPS 2014)*. 143–157.

[24] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2015. The role of social influence in security feature adoption. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. ACM, 1416–1426.

[25] 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 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 1.

[26] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and non-expert attitudes towards (secure) instant messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 147–157.

[27] Janna Lynn Dupree, Richard Devries, Daniel M Berry, and Edward Lank. 2016. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 5228–5239.

[28] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (SEBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2873–2882.

[29] Nicole B Ellison, Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy online*. Springer, 19–32.

[30] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017), 12.

[31] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. 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)*. 59–75.

[32] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of consumer research* 20, 2 (1993), 303–315.

[33] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New me: Understanding expert and non-expert perceptions and usage of the Tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 385–398.

[34] Kathleen Garska. 2018. Two-Factor Authentication (2FA) Explained: Biometric Authentication. `https://blog.identityautomation.com/mfa-face-off-series-biometric-authentication`. (May 2018). Last accessed on: 09.20.2019.

[35] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away from prying eyes: analyzing usage and understanding of private browsing. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 159–175.

[36] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

[37] Tzipora Halevi, James Lewis, and Nasir Memon. 2013. A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 737–744.

[38] Julie M Haney and Wayne G Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 411–425.

[39] Eiji Hayashi and Jason Hong. 2011. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2627–2630.

[40] Cormac Herley. 2009. 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*. ACM, 133–144.

[41] Cormac Herley. 2013. More is not the answer. *IEEE Security & Privacy* 12, 1 (2013), 14–19.

[42] Patrick Houston. 2018. Why Biometrics Are About to Put an End to Password-only Authentication. `https://www.symantec.com/blogs/feature-stories/why-biometrics-are-about-put-end-password-only-authentication`. (Jan 2018). Last accessed on: 09.20.2019.

[43] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 209–223.

[44] Identity Theft Resource Center. 2019. Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). `https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/`. (2019). Last accessed on: 09.14.2019.

[45] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[46] Allen C Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly* (2010), 549–566.

[47] 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 *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 39–52.

[48] Timothy Kelley and Bennett I Bertenthal. 2016. Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites. *Information & Computer Security* 24, 2 (2016), 164–176.

[49] 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).

[50] Issie Lapowsky. 2019. How Cambridge Analytica Sparked the Great Privacy Awakening. `https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/`. (2019). Last accessed on: 09.15.2019.

[51] Robert LaRose, Nora J Rifon, and Richard Enbody. 2008. Promoting personal responsibility for internet safety. *Commun. ACM* 51, 3 (2008), 71–76.

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

[53] Haein Lee, Hyejin Park, and Jinwoo Kim. 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies* 71, 9 (2013), 862–877.

[54] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. 2012. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 589–598.

[55] Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. 2018. Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. In *27th USENIX Security Symposium*. 203–220.

[56] Mary Madden. 2017. Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity. *Data & Society* (2017).

[57] Mary Madden and Lee Rainie. 2015. *Americans' attitudes about privacy, security and surveillance*. Pew Research Center.

[58] Agata McCormac, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson. 2017. Individual differences and information security awareness. *Computers in Human Behavior* 69 (2017), 151–156.

[59] Microsoft. 2019. Microsoft Security. `https://www.microsoft.com/en-us/security`. (2019). Last accessed on: 08.31.2019.

[60] Stefan Palan and Christian Schitter. 2018. Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27.

[61] Odysseas Papadimitriou. 2018. Identity Theft: What It Is, How It Happens & the Best Protection. https://wallethub.com/edu/identity-theft/17120/. (2018). Last accessed on: 09.17.2019.

[62] Simon Parkin, Aad Van Moorsel, Philip Inglesant, and M Angela Sasse. 2010. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop*. ACM, 33–50.

[63] 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 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 295–310.

[64] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 319–338.

[65] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.

[66] 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 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 518.

[67] Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. 2013. Anonymity, privacy, and security online. *Pew Research Center* 5 (2013).

[68] Elissa M Redmiles, Jessica Bodford, and Lindsay Blackwell. 2019. "I Just Want to Feel Safe": A Diary Study of Safety Perceptions on Social Media. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 13. 405–416.

[69] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016a. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, 666–677.

[70] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016b. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[71] 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.

[72] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91, 1 (1975), 93–114.

[73] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. 2015. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *arXiv preprint arXiv:1510.08555* (2015).

[74] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. 2017. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 211–228.

[75] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Second Symposium On Usable Privacy and Security*. 3–4.

[76] 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 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 373–382.

[77] Ruth Shillair, Shelia R Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, and Nora J Rifon. 2015. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 48 (2015), 199–207.

[78] Aaron Smith. 2019. *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*. Pew Research Center.

[79] Geordie Stewart and David Lacey. 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security* 20, 1 (2012), 29–38.

[80] Elizabeth Stobert and Robert Biddle. 2014. The password life cycle: user behaviour in managing passwords. In *Tenth Symposium On Usable Privacy and Security (SOUPS 2014)*. 243–255.

[81] The Cybersecurity and Infrastructure Security Agency. 2019. Tips. https://www.us-cert.gov/ncas/tips. (2019). Last accessed on: 08.31.2019.

[82] The Federal Trade Commission. 2018. Identity Theft. https://www.consumer.ftc.gov/topics/identity-theft. (Sep 2018). Last accessed on: 08.08.2019.

[83] The Federal Trade Commission. 2019a. The Consumer Sentinel Network Data Book 2018. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf. (2019). Last accessed on: 09.19.2019.

[84] The Federal Trade Commission. 2019b. Privacy, Identity & Online Security. https://www.consumer.ftc.gov/topics/privacy-identity-online-security. (2019). Last accessed on: 08.31.2019.

[85] Sabine Trepte, Leonard Reinecke, Nicole B Ellison, Oliver Quiring, Mike Z Yao, and Marc Ziegele. 2017. A cross-cultural perspective on the privacy calculus. *Social Media+ Society* 3, 1 (2017).

[86] U.S. Census Bureau. 2018a. Annual Estimates of the Resident Population by Single Year of Age and Sex for the United States: April 1, 2010 to July 1, 2018. https://www.census.gov/data/tables/time-series/demo/popest/2010s-national-detail.html. (2018). Last accessed on: 09.17.2019.

[87] U.S. Census Bureau. 2018b. Educational Attainment of the Population 18 Years and Over, by Age, Sex, Race, and Hispanic Origin: 2018. https://www.census.gov/data/tables/2018/demo/education-attainment/cps-detailed-tables.html. (2018). Last accessed on: 09.17.2019.

[88] U.S. Census Bureau. 2018c. Households by Total Money Income, Race, and Hispanic Origin of Householder: 1967 to 2018. https://www.census.gov/library/publications/2019/demo/p60-266.html. (2018). Last accessed on: 09.17.2019.

[89] U.S. Census Bureau. 2018d. Population by Age and Sex: 2018. https://www.census.gov/data/tables/2018/demo/age-and-sex/2018-age-sex-composition.html. (2018). Last accessed on: 09.17.2019.

[90] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un) informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 973–990.

[91] Kami E Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2671–2674.

[92] Rick Wash and Molly M Cooper. 2018. Who provides phishing training?: Facts, stories, and people like me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 492.

[93] Rick Wash and Emilee Rader. 2015. Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 309–325.

[94] Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. 175–188.

[95] Rick Wash, Emilee Rader, Kami Vaniea, and Michelle Rizor. 2014. Out of the loop: How automated software updates cause unintended security consequences. In *Tenth Symposium On Usable Privacy and Security (SOUPS 2014)*. 89–104.

[96] Jamie White. 2019. The Nightmarish Experiences of an Identity Theft Victim. https://www.lifelock.com/learn-identity-theft-resources-nightmarish-experiences-identity-theft-victim.html. (2019). Last accessed on: 09.17.2019.

[97] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX Security Symposium*, Vol. 348. 169–184.

[98] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. 2011a. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12, 12 (2011), 798–824.

[99] Heng Xu, Xin Robert Luo, John M Carroll, and Mary Beth Rosson. 2011b. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision support systems* 51, 1 (2011), 42–52.

[100] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2014. Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In *International Conference on Persuasive Technology*. Springer, 302–322.

[101] 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 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 194.

[102] 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 *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 197–216.