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

Yixin Zou*, **Kevin Roundy**†, **Acar Tamersoy**†, **Saurabh Shintre**†, **Johann Roturier**†, **Florian Schaub***
*University of Michigan School of Information †NortonLifeLock Research Group
*{yixinz, fschaub}@umich.edu
†{kevin_roundy, acar_tamersoy, saurabh_shintre, johann_roturier}@symantec.com

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; security and privacy decision-making; adoption; abandonment; technology non-use.

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. Such advice ranges from addressing security risks (e.g., use antivirus software), privacy risks (e.g., opt out of targeted ads), or identity theft risks (e.g., check account statements carefully). However, experts' recommendations are often not adopted by end-users [24, 33, 42, 46, 48].

While prior work has investigated why users adopt or reject expert advice, most studies focused on security practices [34, 48, 74, 75]. Only a few examined privacy practices in specific contexts [1, 36]. Hardly any work has looked into the adoption of identity theft protection practices, despite an increase in privacy and identity theft risks, as evidenced by rising numbers of privacy scandals, data breaches, and financial fraud [47, 53, 90]. Though advice in these areas is increasing, little is known about how and why users adopt or reject privacy and identity protection practices. Moreover, most prior work on advice adherence has focused on motivations and hurdles for initial advice adoption [34, 48, 80]. 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 re-freeze 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, or abandoned? (RQ2) *What* are predictive factors for 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, covering 30 expert-recommended security, privacy and identity theft protection practices suggested by prior work [17, 48, 60, 89]. Security practices were more widely adopted than privacy and identity theft protection practices. Both manual practices (i.e., users need to remember to adhere to the practice) and automated practices (i.e., no user effort 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 discounting warnings from security tools. 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

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

ACM ISBN 978-1-4503-6708-0/20/04 ...$15.00.
http://dx.doi.org/10.1145/3313831.3376570

and identity theft protection tools to promote such adherence, especially when recurring user interaction is required.

RELATED WORK

We discuss prior work on expert advice and its communication to users, usability issues with existing tools, and 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, 18, 50], but behave insecurely sometimes [29]. A variety of online safety advice for consumers is provided by corporate (e.g., [21, 22, 63]) and government entities (e.g., [88, 91]). Many organizations mandate employee training prior to receiving network or computer access [31]. Yet substantial discrepancies exist between security practices of experts and non-experts, suggesting that the communication of expert advice could be improved [17, 48]. Expert advice is often vague, unrealistic, or contradictory [76], and might not be economically rational, e.g., time spent checking URLs might exceed potential monetary loss from phishing [43]. Improving expert advice requires keeping up with evolving attack vectors, empirically evaluating advice's socioeconomic outcomes, and a deep understanding of human behavior and effective risk communication [41, 43, 44, 76].

Security and Privacy Decision Making

Rational choice theory views humans as rational agents, suggesting they would only follow advice when benefits (e.g., protection from potential harm) exceed costs (e.g., effort to implement the advice) [4]. Thus, one reason for rejecting security advice one's *compliance budget*, i.e., one can only devote limited time and resources to security behavior [13, 67]. Indeed, some studies find that users carefully weigh costs and benefits in choosing strategies to cope with security risks [34, 80]. Similarly, *privacy calculus* theory argues that users disclose information online when perceived benefits (e.g., social validation, social capital gains) outweigh privacy loss [32, 56, 86, 92, 107].

Psychology-based theories also help explain security and privacy decisions. The *theory of planned behavior* [6] identifies the importance of attitudes, subjective norms, and perceived behavioral control. *Protection motivation theory* [77] suggests that threat perception and subjective assessment of coping mechanisms are crucial to forming the intention to act, and has been widely applied [9, 23, 49, 84, 106]. Research based on *social cognitive theory* [11] highlights how security and privacy behavior is influenced by observations of others, and advice received from trusted peers or media [24, 26–28, 75].

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 context-dependent, and malleable [3]. More sensitive information is disclosed when it is perceived as social norm, but also when more privacy controls are provided [5, 15]. Similarly, security decisions are subject to overconfidence and optimism bias, such as in the wake of data breaches [110].

Demographic factors, prior knowledge and experience also affect security and privacy behavior. Women tend to be more susceptible to phishing than men [40, 83]. Younger people, despite heavier social media use and disclosure, engage more actively in privacy-protective behaviors [52, 72]. People with lower incomes might struggle to identify protective tools and strategies, often due to limited online access [46, 59, 74]. More knowledge is generally correlated with higher risk sensitivity and intention to adopt safe practices [54, 71]. Yet objective knowledge can be overwritten by users' inherent beliefs [100], such as "no matter what I do, I won't be 100% secure" [75, 80], and "I've got nothing to lose" [110]. More educated users, while holding more sophisticated beliefs, also tend to take fewer precautions [101].

Usability Issues with Existing Tools

Usability issues are a key contributor to partial adoption or rejection of online safety practices. Password managers' usability issues (e.g., no support for biometric authentication, long setup time) create adoption barriers [7, 8]. For two-factor authentication (2FA), users may feel its usability costs outweigh security improvements [20]. Tools that limit tracking and targeted advertising suffer from confusing interfaces, broken links, and insufficient feedback [39, 57, 81]. Usability issues persist with email encryption and key management [79, 105]. Secure mobile messaging apps simplify key management, but adoption is still limited by fragmented user bases [1].

Compared to security and privacy tools, the usability of identity theft protection services has received little attention. In scenario-based experiments [78], only 6% of participants reported paying for an identity theft protection service, but respective reasons are not clear. Usability issues also emerge in measures dealing with data breach protection, such as having to retain a PIN to lift a credit freeze [110].

Abandonment of Security and Privacy Practices

Technology abandonment or non-use is a poorly-understood phenomenon in general, with some research in specific contexts, such as instant messaging [14], mobile games [103], and social media [12]. Common reasons of technology abandonment among these studies include ongoing monetary costs (e.g., in-app purchases), functionality failing expectations, and annoyance from unwanted social interactions [12, 14, 103]. It is unclear whether these generalize to online safety practices.

Usability issues appear to drive abandonment of a technology by not only creating adoption barriers but also affecting user experience afterwards. For instance, password managers were abandoned when they failed to store passwords accurately [69]. Secure communication tools were abandoned due to low quality of service [1]. Users who had a bad updating experience were less inclined to update that software in the future [98]. For virtual private networks (VPNs) however, emotional considerations (e.g., fear of surveillance) play a key role in overcoming usability issues and encouraging continued engagement [64]. Our study contributes 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 assess adoption and abandonment of expert-recommended practices, 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 by consumers; what factors influence levels of adoption; and reasons for partial adoption or abandonment. A survey allows us 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 the University of Michigan's Institutional Review Board.

Taxonomy of Expert-Recommended Practices

We conducted an extensive literature review to determine which expert-recommended practices to include (see Table 1). Prior work mostly associates online safety with security measures [48], but privacy and identity theft risks are increasing, making it important to contrast and characterize user adherence to expert advice regarding these adjacent domains.

The chosen security practices (n=12) were primarily based on Ion et al.'s 2015 study on security advice [48]. They surveyed >200 experts (5+ years computer security work experience) about their top three pieces of online security advice for non-tech-savvy users. Most expert advice remained constant in Busse et al.'s 2019 replication study [17]. We studied the 11 most-mentioned practices (of 152 total) in our survey, as they are likely to be agreed on by most experts [76]. Following the authors' recommendation [76], we replaced one of those practices ("be careful/think before you click") with two ("don't click links in email from unknown sender" and "check URL for expected site"), resulting in 12 security practices in total.

Because no comparable systematic elicitation of expert advice existed for privacy and identity theft protection practices, we broadened our search to online articles, reports, and blog posts by experts from industry, government, and NGOs. Our chosen privacy practices (n=12) were primarily based on a census-representative 2015 Pew survey examining Americans' attitudes and behaviors about privacy [60], which asked whether respondents had engaged in any of 13 privacy-enhancing practices. We included all but two of those practices ("delete/edit something posted in the past" and "ask someone to remove something posted about you"), for which consistent and frequent full adoption might not be applicable or practical. We added the practice of opting out of facial recognition to unpack users' respective behaviors given its substantial privacy implications [19, 85].

Our chosen identity theft protection practices (n=6) came from the Federal Trade Commission [89]. We included practices clearly focused on identity theft protection and excluded more general security/privacy practices (e.g., "don't overshare on social networking sites") and practices that only apply to victimized individuals (e.g., identity recovery services). Notably, some practices like credit freeze (restricting access to one's credit report at a credit bureau) are only available to U.S. consumers. As such, we only recruited U.S. participants to control cultural differences.

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. **Security practices S1-S12 obtained from [17, 48, 76], privacy practices P1-P11 from [60] and P12 from [19, 85], and identity theft protection practices I1-I6 from [89].

Table 1. Security, privacy, and identity theft protection practices included in our study.

In developing our practice taxonomy, we noticed that practices varied in the level of required user involvement, which may explain differences in adoption and abandonment. *Manual* practices require users to remember to adhere to the practice and implement it on their own (e.g., avoiding clicking links sent by unknown people) – success of the practice solely relies on users' manual application and cognitive assessment. *Automatic* practices instead constitute the adoption of a particular tool or service that, after initial setup, provides automatic protection with minimal user involvement (e.g., using an ad blocking extension). *Assisted* practices, like 2FA, require the adoption of a tool or service but users also need to interact with them recurrently for full protection.

Survey Protocol

We conducted our study on Prolific, a crowdsourcing platform similar to Amazon Mechanical Turk but provides more demographically diverse participants [65, 70]. We described the survey topic as "risk management when using the Internet" to reduce self-selection bias by avoiding priming about security, privacy, or identity theft. We recruited U.S. participants who were 18 years or older with a >90% approval rate. Participants were compensated $1.20 for work that took 5-10 minutes (mean: 9.68, median: 7.34), in line with Prolific's required minimum hourly pay.

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 Qualtrics 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 to minimize respondent fatigue. An attention check question was randomly placed among the 10 practices.

We used the question format "Have you ever...?" for all practices. We provided definitions of terms, tools, or services involved for practices that might not be immediately comprehensible to the general public, and provided screenshots of relevant UI elements for some practices to reduce chances of misconception and confusion (denoted by * in Table 1). For each practice, we asked participants if they have *fully adopted*, *partially adopted*, *abandoned*, *considered*, *rejected*, *not understood* the given practice, or something else (*other*). See Table 2 for the full response option texts. For four practices, we further clarified response choices to help participants distinguish between full and partial adoption (e.g., defining "full adoption" as "making multiple requests throughout the year" for obtaining free credit reports), or when partial adoption did not apply to the practice (e.g., one either signs up for credit monitoring service or not).

After going through the 10 practices, participants were asked about prior experiences with unauthorized account access, data breaches, and identity theft. The survey concluded with demographic questions about age, gender, income, education, employment, and background in computer science (CS)/information technology (IT), and security/privacy. A "prefer not to answer" choice was offered for potentially sensitive topics. The full survey is included in this paper's online supplemental material.

Data Analysis

After removing 17 participants who failed the attention check question, we received 902 complete survey responses. The sample size followed the rule of thumb for linear mixed-effect models – at least 1,600 observations per condition in designs with repeated measures [16].

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 read all responses and developed codes using inductive coding [55]. Two co-authors then independently analyzed 150 (8.7%) randomly sampled responses, reconciling codes and revising the codebook iteratively until reaching high inter-coder reliability (Cohen's κ=.82). The two co-authors then split the dataset and single-coded all responses. Our codebook is included in the supplemental material.

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 placing a 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 re-coded these responses to minimize report biases and inconsistencies in the data. In total, 171 responses were re-coded, of which 75 were originally *abandonment*, 71 were *other*, and 25 were *partial adoption*.

Statistical analysis

Using the re-coded dataset, we calculated descriptive statistics for each practice's rates of full adoption, partial adoption, abandonment, etc. Motivated by prior work suggesting the influence of user characteristics and tool usability issues on user behavior, we constructed mixed-effect regression models. For fixed-effect factors, we included characteristics related to the user (i.e., demographics, technical background, prior negative experience) and the practice (domain and 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) [62] for all models are below .20, indicating that random differences between individual participants or practices contributed little to variances in the adoption level.

To understand what factors influence users' current levels of adoption, 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*. Results are reported in Table 4. Since the response options are only quasi-linear, we also ran ordinal logistic regressions to validate linear regression results, which produced the same findings with only minor variations in numeric outputs of effect size. Thus, we report linear regression results only since they are more informative. To know how effects of different predictors vary across security, privacy and identity theft domains, we further ran a series of models, each adding interaction terms between practice domain and another predictor (e.g., interaction terms between practice domain and gender show how gender effects on adoption vary across domains). Post-hoc power analyses suggest that our study was sufficiently powered: based on 1k simulations of the likelihood ratio test, the power to detect the overall effect of the domain variable on adoption is 97.20%, CI (95.98%, 98.13%).

To understand what factors influence a practice being abandoned, we tried running logistic regressions on a binary variable with "yes" meaning *abandonment*, and "no" meaning *partial adoption* or *full adoption*, excluding other response

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 [93–96].

options. However, due to the small number of abandonment cases in our dataset (534 "yes," 5,325 "no") the model expectedly failed to converge. Similarly, multinomial logistic regressions on the full spectrum of response options failed to converge because response options like "unaware" and "other" were much less frequent than others. Therefore, our regression analysis only focuses on adoption and we refrain from making statements about which variables are correlated with abandonment, consideration, or other response options.

Limitations

While our scope of investigated practices exceeds most prior work, there might be other relevant practices related to security, privacy, identity theft protection, or other online safety topics, such as harassment and cyberbullying [73] worthy of future study. Additionally, as with any survey, participant may over-report their behavior due to social desirability bias [35]. This effect may be particularly salient for *full adoption* when participants think they consistently implement a practice while forgetting exceptions they make. 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 removal of partial adoption as a response option 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 reduce confusion in the survey, as partial adoption is not applicable to these practices.

RESULTS

Below we describe our participant sample, discuss 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. population 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. Of our participants, 66.6% had no background in CS/IT or security/privacy; 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.

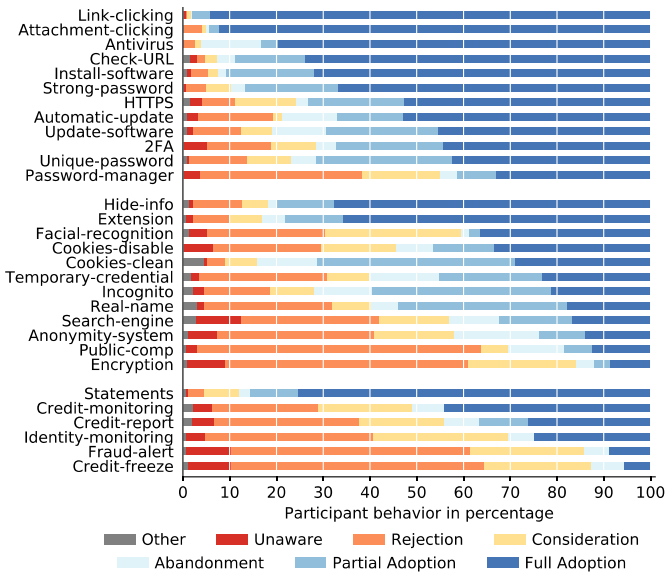

Figure 1. Distribution of response options for each practice. The practices are sorted by full adoption rates in descending order.

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 many participants reported they would not consider them.

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 hiding information that is not essential to transactions (69.0%) and using a privacy-enhancing browser extension (68.0%). Checking account statements was the only identity theft protection practice that was fully adopted by over half of participants (76.2%). Except for antivirus software and privacy extensions, 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 security and privacy, with the top three being about privacy risk management (49.7% for cleaning cookies, 39.9% for incognito, 39.1% for avoiding websites asking for real names). Consistent with prior work [58, 68, 87], a substantial proportion of participants did not fully follow expert-recommended password management practices (29.4% for unique passwords, 21.4% for strong passwords).

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 using an anonymity system such as VPN most commonly abandoned (16.8%). Using automatic updates for software (13.3%) and antivirus (11.0%) were the most abandoned security practices. 7.2% had abandoned a credit monitoring service. Some abandonment decisions appear rational, since they seem more realistic for one-time use rather than long-term implementation (e.g., using a public computer for anonymous browsing). Yet some other abandoned practices such as cleaning cookies do require consistent implementation for effective protection.

Low adoption/acceptance of practices against identity theft

Among practices that had not yet been adopted by most participants, many pertain to identity theft risk mitigation. The top practices considered for future implementation were opting out of facial recognition (29.2%), using an identity monitoring service (28.9%), and placing a fraud alert (24.6%). Most of these require adopting tools or services, either automated ones (e.g., credit/identity monitoring) or tools that 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 [109].

RQ2: Factors Affecting Levels of Adoption

Our mixed-effect linear regression models show that different levels of adoption are related to the practice's domain and its type of user interaction. We further found significant effects on adoption from demographics, technical background, and prior negative experiences. Results of the main regression model are shown in Table 4.

Levels of adoption: security > privacy ≥ identity theft

Confirming the descriptive analysis, the adoption level of security practices was significantly higher than those for privacy practices or identity theft protection practices. While privacy practices exhibit higher levels of adoption than identity theft protection practices, the difference is not significant.

Low adoption for recurring interaction practices

We were interested in whether a practice's degree of user interaction (manual, assisted, automated) affects adoption. We expected 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 and automated practices exhibiting significantly higher levels of adoption. The difference between manual and assisted practices was particularly salient for identity theft practices (b=1.02, CI=[.40, 1.64], p<.001), but such significant difference does not persist for security or privacy practices alone.

Gender and age differences in levels of adoption

We further identify significant effects on adoption levels from certain user characteristics. Men had significantly higher levels of practice adoption compared to women. Such gender difference applies to security and privacy practices in particular (b=.11, CI=[.04, .17], p<.01 for both). This confirms prior work showing similar gender difference for phishing susceptibility [40, 83] and extends it to a wider range of practices.

Mapping age to the following categories: 18-34, 35-54, and 55+, we find significant age effects for security and privacy practices, but not overall. Middle-aged participants (35-54) adopted more security practices than younger participants (b=.07, CI=[.01, .14], p<.05). This aligns with prior finding [61] that older people 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, CI=[.07, .20], p<.001) and older participants (b=.23, CI=[.13, .33], p<.001). This extends prior finding that young adults are more likely to engage in privacy-protective behaviors on Facebook [52] to other privacy practices.

Higher adoption among low-income participants

Mapping household income to the categories <$50k, $50-100k, and >$100k, we find the overall trend 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, CI=[.04, .22], 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 prior finding that people with lower incomes have heightened informational and physical privacy and security concerns [59], which might translate into the adoption of protective practices that are accessible and affordable to them.

More education contributed to higher adoption

Mapping educational background to the categories less than Bachelor's degree, Bachelor's degree or equivalent, and graduate degree, we find that more educated participants exhibited higher levels of practice adoption overall. In particular, participants with a Bachelor's degree (b=.24, CI=[.15, .33], p<.001) or a graduate degree (b=.34, CI=[.21, .45], p<.001) had significantly higher adoption of identity protection practices than those without. Compared to prior finding that more educated people tend to take fewer security precautions [100], our work suggests that the trend might be different for mitigating identity theft risks.

Category	Variable	*b*	CI	Original p-value	Adjusted p-value
Age	18-34	-	-	-	-
	35-54	.00006	[-.05, .05]	.99	.99
	>55	-.04	[-.12, .03]	.26	.33
Gender	Women	-	-	-	-
	Men	.08	[.04, .13]	<.01 (**)	<.01 (**)
	Non-binary	0.08	[-.09, .25]	.36	.43
Income	<$50,000	-	-	-	-
	$50,000-$100,000	-.03	[-.08, .02]	.23	.33
	>$100,000	-.06	[-.13, .004]	.07	.13
Education	No Bachelor's degree	-	-	-	-
	Bachelor's degree	.05	[.002, .10]	<.05 (*)	.09
	Graduate degree	.02	[-.06, .09]	.66	.74
Tech background	Neither IT nor S&P	-	-	-	-
	Only IT	.09	[.02, .16]	<.05 (*)	<.05 (*)
	Only S&P	.07	[-.01, .15]	.09	.16
	Both IT and S&P	.15	[.08, .22]	<.001 (***)	<.001 (***)
Prior experience	Unauth. access: No	-	-	-	-
	Unauth. access: Yes	-.01	[-.06, .04]	.70	.74
	Data breach: No	-	-	-	-
	Data breach: Yes	.05	[.002, .10]	<.05 (*)	.09
	Identity theft: No	-	-	-	-
	Identity theft: Yes	.16	[.10, .23]	<.001 (***)	<.001 (***)
Privacy domain	Identity	-	-	-	-
	Privacy	.20	[-.11, .50]	.21	.33
	Security	.62	[.31, .94]	<.01 (**)	<.01 (**)
Practice nature	Assisted	-	-	-	-
	Automatic	.53	[.21, .85]	<.01 (**)	<.01 (**)
	Manual	.64	[.37, .90]	<.001 (***)	<.001 (***)

"-" means the variable is set as the baseline in the model. Comparisons between any pairs of non-baseline variables in this table were also made, and results are reported in text. The regression coefficient (*b*) shows to what extent the variable, compared to the baseline, brings the outcome (level of adoption) up or down on a scale from 0 to 2. CI is the 95% confidence interval. Statistically significant factors (adjusted p<0.05 after applying the Bonferroni-Holm correction) are denoted with *.

Table 4. Results of the main regression model, excluding interaction terms between the practice domain and other variables.

11% of participants reported a background in both 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. Interestingly, this difference between experts and non-experts holds true when considering CS/IT only, but not for participants who reported a background only in security/privacy (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-ended responses, was mostly based on university courses or employer-mandated trainings.

Experiencing identity theft contributes to high adoption

Overall, participants who had prior experience with identity theft incidents adopted more protection practices. This trend also holds true when looking at security, privacy, or identity theft practices individually, suggesting it is a robust trigger for pro-safety behaviors (b=.14, CI=[.05, .23], p<.01 for security; b=.11, CI=[.01, .20], p<.05 for privacy; b=.33, CI=[.21, .45], p<.001 for identity). Experience with being a victim of data breaches is also correlated with higher levels of adoption, though the effect is non-significant. By contrast, experience with unauthorized access to online accounts has little impact on adoption levels.

Partial Adoption	Count	Abandonment	Count
site-specific	179 (15%)	not-needed	68 (20%)
only-sensitive	129 (11%)	because-of-risk	50 (14%)
impractical	124 (10%)	impractical	41 (12%)
own-judgment-sufficient	111 (9%)	usage-interference	23 (7%)
because-of-risk	95 (8%)	own-judgment-sufficient	21 (6%)
usage-interference	80 (7%)	using-substitute	21 (6%)
only-finance	74 (6%)	platform-specific	17 (5%)

Table 5. Top coded reasons for partial adoption and abandonment.

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 5. Tables 6 to 8 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* (e.g., "I do this sometimes").

Reasons for partial adoption

As shown in Table 5, 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 avoiding websites that ask for real names (57 participants) and using temporary credentials for online activities (31). Unfortunately, most participants did not specify where they applied the practice selectively. For those who did, 129 (11%) did so for sensitive sites (*only-sensitive*), 74 (6%) for finance-related sites (*only-finance*), 41 (3%) for suspicious or odd sites (*only-suspicious*), 15 (1%) for social media services (*only-social-media*), and 5 (<1%) for gaming services (*only-gaming*). For practices adopted when visiting sensitive sites, 47 participants reported that they used incognito mode to interact with sensitive websites (e.g., adult sites, dark web), in line with prior work [38]. Other privacy practices were also adopted for this reason, though less frequently, such as using an anonymity system like VPN (8) or a search engine that does not track search history (8). Some mentioned taking extra precautions for finance-related sensitive information: 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"), updating software immediately ("if I am in the middle of something I will not [do it]"), and using unique passwords ("it's hard to keep track"). Inconvenience extended to privacy practices, including cleaning cookies (12, e.g., "it kills all my passwords") and using incognito mode (11, e.g., "I like to be able to have a list of the places I visited if I need to go back"). A few 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%) reported relying on their 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), disabling automatic update for software at times (10), and clicking unknown attachments (5). For example, in talking about clicking attachments, one participant said: "I don't click on obvious spam emails, but I am willing to open emails that seem legitimate even if I don't know the senders," which is concerning given that even trained individuals routinely fall for phishing emails [83]. Similar trends manifested for privacy practices, with 9 participants disclosing non-essential information 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 checking account statements for fraudulent charges (21) and obtaining credit reports (6). The at-risk feeling also motivates use of strong passwords (11) and anonymity systems (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/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 updating software (23), using privacy-enhancing browser extensions (17), and disabling third-party cookies (12). Users selectively abandoned updates when buggy updates had "broken drivers, programs, or the OS itself" (in line with [98]), 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 5. 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, it was particularly salient for privacy practices, with 5 of 10 privacy practices abandoned most likely because their value was not recognized (see Table 7). 4 of the 5 practices pertained to browsing activities, with the following comments on using incognito mode 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 cases (14%) participants abandoned a practice after perceiving that risk levels had diminished (*because-of-risk*). This justification was the dominant reason for abandoning a fraud alert or credit freeze, which were commonly adopted after a fraud or lost/stolen credit card incident and dropped soon afterwards. Similarly, 11 participants had used temporary credentials for online activities 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 online, 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 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 disabling third-party cookies (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 managers were 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 [68].

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 [24, 46] and expert advice is often vague, inactionable, and contradictory [44, 76]. 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

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 6. 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-social-media (3), platform-specific (2), forgetting (1)	1	unapplicable

Table 7. Participants' most frequent reasons for incomplete adoption and abandonment of privacy practices.

concerning given that practices from different domains often intersect. For example, phishing is a common attack vector for identity theft [66]. Manual security practices (e.g, avoid clicking unknown links) are prone to cognitive errors and inconsistent application, in which case assisted security such as 2FA and identity theft protection practices (e.g., credit freeze and 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 [17, 48]. However, 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 [24]. We find 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 [109]. Similar to phishing training materials [99], 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 [104]) 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. From our qualitative analysis, some participants reported following 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., abandoning incognito mode when device is not shared). Yet interventions are needed when perceptions of decreased risk are misaligned with objective risks. For instance, some participants abandoned credit freezes and fraud alerts soon after data breaches, even though the objective identity theft risks may not change over time once sensitive information has been exposed. Thus, 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.

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 8. Participants' most frequent reasons for incomplete adoption and abandonment of identity protection practices.

Tailor advice to audience characteristics

Prior research suggests a "digital divide" in security and privacy: people with less education and lower socioeconomic status may have access to fewer resources, exposing them to further vulnerability [51, 74]. Our findings are more nuanced. More technology knowledge is linked with higher levels of practice adoption. Interestingly, security/privacy expertise alone had no effect. 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 [59]. Notably, most of our investigated privacy practices are free or have free options (e.g., anonymity systems such as VPN). These results confirm the need for expert advice to be tailored to specific audiences to be effective [59]. For instance, the use of personas [30] and scenarios reflecting different audiences and their needs could help users identify solutions most suitable to them, yet they need to be crafted carefully to be inclusive.

Implications for Design

Building on prior work, our study indicates that usability issues exist widely across security, privacy, and identity theft protection practices, and function as a key contributor to partial adoption and abandonment. While usability research has largely focused on security practices, usability of privacy and identity protection practices requires 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

In line with prior work [68, 69, 98, 102, 108], we identify usability issues as a key contributor to partial adoption and abandonment across different practices, such as updating software, using a password manager, and using unique passwords. Users may partially or fully abandon a practice when it is difficult and inconvenient to implement, sometimes reaching the level of disrupting the normal user experience, even when they recognize the practice's value. While prior work has primarily advocated for improving the usability of assisted security practices such as 2FA [25], more usability research is needed for frequently abandoned or rejected privacy and identity protection practices to lower their barriers for adoption. Browsing-related privacy practices in particular show significant usability issues and deserve more attention. For instance, cleaning browser cookies was considered impractical as it also removes desired cookies (e.g., session and login cookies). Similar to purpose-oriented cookie consent banners [97], 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 manual practices we investigated are primarily 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 shown by our results. Conversely, most assisted practices (e.g., anonymity systems and password managers) generally require some level of expertise for initial setup, which may scare non-tech-savvy users away [8, 69], or have known usability issues that significantly impact user experience [79, 82].

For tool-based practices such as using a password manager, their features and functionality need to be better communicated to prospective users to dispel identified misconceptions. Required user effort should also be reduced where possible. For instance, most participants who adopted password managers 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 [44]. 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 [37, 45]. 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.

ACKNOWLEDGEMENTS

Yixin Zou's work was partially supported by a NortonLifeLock Graduate Fellowship. The authors thank Abraham Mhaidli, Joey Hsiao, Justin Petelka, Oliver Haimson, and Qiaoning Zhang for feedback on earlier versions of this paper, as well as all members of the NortonLifeLock Research Group and the U-M Security Privacy Interaction Lab for their kind support.

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] Eric Baumer, Phil Adams, Vera D. Khovanskaya, Tony C. Liao, Madeline E. Smith, Victoria Schwanda Sosik, and Kaiton Williams. 2013. Limiting, leaving, and (re)lapsing: an exploration of facebook non-use practices and experiences. In *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems*.

[13] 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.

[14] Jeremy Birnholtz. 2010. Adapt, Abandon: Understanding Why Some Young Adults Start, and then Stop, Using Instant Messaging. Computers in Human Behavior 26(6), 1427-1433. *Computers in Human Behavior* 26 (11 2010), 1427–1433.

[15] 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.

[16] Marc Brysbaert and Michaël Stevens. 2018. Power analysis and effect size in mixed effects models: A tutorial. *Journal of Cognition* 1, 1 (2018).

[17] 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)*.

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

[19] 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.

[20] 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.

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

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

[23] 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.

[24] 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.

[25] 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*.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] 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.

[37] 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.

[38] 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.

[39] 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)*.

[40] 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.

[41] 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.

[42] 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.

[43] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop*. ACM, 133–144.

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

[45] 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.

[46] 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.

[47] 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.

[48] 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.

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

[50] 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.

[51] 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.

[52] 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).

[53] 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.

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

[55] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human-computer Interaction*. Morgan Kaufmann.

[56] 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.

[57] 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.

[58] 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.

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

[60] Mary Madden and Lee Rainie. 2015. *Americans' Attitudes about Privacy, Security and Surveillance*. Pew Research Center.

[61] 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.

[62] Kenneth O McGraw and Seok P Wong. 1996. Forming inferences about some intraclass correlation coefficients. *Psychological Methods* 1, 1 (1996), 30.

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

[64] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P. Knijnenburg. 2020. Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proceedings on Privacy Enhancing Technologies Symposeum (PoPETS)* 1 (2020).

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

[66] 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.

[67] 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.

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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).

[73] 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.

[74] 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.

[75] 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.

[76] 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.

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

[78] Heather Rosoff, Jinshu Cui, and Richard John. 2014. Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. In *Tenth Symposium On Usable Privacy and Security (SOUPS 2014)*. 175–186.

[79] 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).

[80] 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.

[81] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. 2016. Watching Them Watching Me: Browser Extensions' Impact on User Privacy Awareness and Concern. In *Workshop on Usable Security (USEC)*.

[82] 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.

[83] 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.

[84] 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.

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

[86] 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.

[87] 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.

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

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

[90] 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.

[91] 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.

[92] 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).

[93] 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.

[94] 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.

[95] 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.

[96] 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.

[97] 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.

[98] 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.

[99] 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.

[100] 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.

[101] 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.

[102] 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.

[103] Pei-Shan Wei, Szu-Ying Lee, Hsi-Peng Lu, Jen-Chuen Tzou, and Chien-I Weng. 2015. Why Do People Abandon Mobile Social Games? Using Candy Crush Saga as an Example. *International Journal of Industrial and Manufacturing Engineering* 9, 1 (2015), 13 – 18.

[104] 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.

[105] 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.

[106] 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.

[107] 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.

[108] 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.

[109] 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.

[110] 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.