A Survey of User Experience in Usable Security and Privacy Research

Danielle Jacobs[1(✉)] and Troy McDaniel[2]

[1] School of Computing and Augmented Intelligence, Arizona State University,
Tempe, AZ 85281, USA
danielle.r.jacobs@asu.edu

[2] The Polytechnic School, Arizona State University, Mesa, AZ 85212, USA
troy.mcdaniel@asu.edu

Abstract. Today people depend on technology, but often do not take the necessary steps to prioritize privacy and security. Researchers have been actively studying usable security and privacy to enable better response and management. A breadth of research focuses on improving the usability of tools for experts and organizations. Studies that look at non-expert users tend to analyze the experience for a device, software, or demographic. There is a lack of understanding of the security and privacy among average users, regardless of the technology, age, gender, or demographic. To address this shortcoming, we surveyed 47 publications in the usable security and privacy space. The work presented here uses qualitative text analysis to find major themes in user-focused security research. We found that a user's misunderstanding of technology is central to risky decision-making. Our study highlights trends in the research community and remaining work. This paper contributes to this discussion by generalizing key themes across user experience in usable security and privacy.

Keywords: Cybersecurity · Human factors · Information security · Privacy · Usability

1 Introduction

Modern technology allows users to be connected, and as a result, so much of daily life depends on technology. This dependency is deepening as smart connected devices continue to drive transformative changes to the digital age, putting individuals' privacy at risk. The risk to users is sizeable, covering the gamut from company data breaches, hardware-level vulnerabilities that leak passwords, to poor security hygiene that gives information away. Moreover, the widespread adoption of technology increases these risks, as demonstrated by the recent upsurge in cybercrime [33]. The field of usable security and privacy was developed in response to ubiquitous technology's emerging threats. According to NIST, the

The authors thank Arizona State University and the National Science Foundation for their funding support under Grant No. 1828010.

A. Moallem (Ed.): HCII 2022, LNCS 13333, pp. 154–172, 2022.
https://doi.org/10.1007/978-3-031-05563-8_11

research aims to "make it easy to do the right thing, hard to do the wrong thing, and easy to recover when the wrong things happen" [51]. Furthermore, we want to design technology, especially security and privacy-focused solutions, to be user-friendly. A cross-discipline approach helps to inform solutions. This area's interdisciplinary research spans hardware, software, human-computer interaction, psychology, economics, and more. Such collaborative research builds a collation to understand better the dynamics of technology, end-users, security, and privacy.

An integrative approach to user-centered privacy and security is not new. By the 1980s, researchers were applying human factors to privacy and security [22]. With nearly 40 years of progress, it is essential to pause and examine the efforts. There is a myriad of publications to survey. Understanding the gaps, current state, and everyday experiences of the user can provide a foundation for continued progress. The scope of current work is prodigious, partly due to the decades of work and multi-disciplinary methods. The usability of technology has been an evolving process. In the late 1980s, Karat studied security usability through the lifecycle of a tool's development [22].

Today, looking at the existing work, we see a variety of tools and technologies. Researchers have sought to understand how the privacy and security of everyday tools can better address issues faced by users. This includes determining cognitive models users create when engaging with tools and highlighting existing knowledge gaps. Overall we see the main focus of current work centered around certain groups of users or technology applications. A large subsection of this work includes deep dives into studying experts, resulting in the identification of themes as part of a qualitative review of nearly 70 publications to better capture how researchers define the field [28]. More specific to end-users, we see some work describing how users react to vulnerabilities, focusing on novice users' processes [5,39]. Surveying the current publications for usable security and privacy, we found a heavy focus on organizations, specialists, specific demographics, or particular technologies. We may understand how security researchers and experts define the risks and the field of study. However, there has been no effort to generalize a user's understanding of usable security and privacy.

This review dives deep into existing literature to extract and analyze how novice users perceive security and privacy. First, we will investigate the findings from the literature to find common themes in user experience across technology. Next, we will apply a qualitative data analysis technique to identify the end-user-specific themes. In analyzing the data, we will answer questions around the research community and user experience. Finally, this review highlights emerging trends and questions in the area. We seek to answer the following research questions (RQ) to guide our research:

RQ1 [User Experience and Risk]: *What user behaviors put users more at risk, and what do users believe places them most at risk?*
We found several responses, thoughts, and situations users shared across the surveyed studies. Diving deeper into what was reported in the citations, we found that misunderstandings and design issues cause risky behaviors.

We document examples of risky behavior across the literature through the coding process and showcase examples. In our findings, the misconception of technology, tool design, and trust leads users to make more risky decisions.

RQ2 [Trends and Challenges]: *What are emerging trends and challenges to the field?*
There are several common approaches to study usable security and privacy. Our results show surveys, interviews, and user experiments are the most common methods applied to research. We also illustrate trends in researched topics across the papers. Three topics are explored the most: warnings, phishing attacks, and passwords. More recent publications suggest an emerging trend in the heterogeneity of user groups, as articles consider different demographics. This highlights the communities' realization that security and privacy tools need to meet a diverse population. Furthermore, we report on the challenges and future work based on the surveyed literature. These challenges are reported as a series of themes. We find that there are discrepancies between future work and challenges. Finally, in looking at the remaining gaps, we discuss the most cited obstacles and emerging issues that remain.

2 Related Work

Here we briefly review the current topics covered around usable privacy and security. Finally, we describe how our work is different from work that has come before.

2.1 Usable Security and Privacy Work

Work in usable security and privacy has been around since the 1980s. In the 90s, Whitten and Tygar looked at how the usability of PGP 5.0 prevents the average person from adopting encryption software [56]. With the threat landscape growing for cyber physical systems, corporations, and governments, a plethora of work has looked at cybersecurity from the perspective of a larger system [15,35,52]. In this context, usability is especially important for response and operations.

For example, Kokulu et al. investigated Cybersecurity Operations Centers (SOC) to find common operational bottlenecks that can be addressed to improve a SOC's effectiveness [23]. In other recent papers, researchers apply situational awareness to the cybersecurity incident responders [2]. Others have sought to integrate usability to develop better tools for security response, making analysis easier [18]. This shows the diversity of current work. While there is vast work on improving security usability for specialists and organizations, another breadth of research focuses on the everyday user.

Prior work has sought to understand users' perceptions and experiences with data usage. Work that focuses on user experience has converged on understanding difficulties users have with integrating security and privacy into everyday life.

For example, Schufrin et al. created TransparencyVis to allow users to visualize how personal data is used online [47]. Instead of looking at data for privacy, some work has focused on a specific technology's usable security and privacy. Sunshine et al. set out to understand how helpful SSL warnings are to users [53]. In addition, several recent works examine factors that influence security behaviors. Pearman et al. looked at the challenges in adopting password managers [36]. Ray et al. built from Pearman et al.'s work and examined challenges facing password managers for older adults [38]. Similarly, researchers have examined the impact of specific demographics in usable security and privacy [31,42,50]. Usable security and privacy research ranges from visualizations to user's mental models. Motivated by a citizen-centered, end-user-centered approach, this paper focuses specifically on research that targets the average user.

Qualitative Coding. Lennartsson et al. perform a literature review of what usable security means to the research community to capture this breadth better [28]. In this piece, Lennartsson et al. apply qualitative coding to a large sample size of usable security and privacy research to identify novel themes that impact usability for security-related topics. We expect to see some differences and similarities for our user experience-focused analysis. This is because our survey paper specifically focuses on the everyday end-user and our research questions.

Framework. Prior work has examined the human factors surrounding everyday users' reactions to vulnerabilities [39]. Rebensky et al. focused on two areas. First is the stages of human response to cybersecurity events. The second is factors that influence human response to cybersecurity events. This resulted in formalizing developed cybersecurity response factors.

Contribution. Our research contrasts with prior work by expanding the meta-analysis. A key contribution to the field is our assessment of trends, challenges, and future opportunities. In addition, we seek to better understand the themes reported around user experience and other aspects of existing work.

3 Methods

This analysis explores usable security and privacy research around the everyday user. By understanding the trends, patterns, user-oriented results, and remaining gaps, researchers can direct efforts toward solving remaining challenges. End-user-centered research is a broad field. Therefore, this paper excludes citations concentrating on organizational and security experts to narrow the scope and provide a survey paper centered on everyday users. The motivation of this survey is first to examine research from the lens of a security researcher and second from the perspective of a human factors researcher. The selected literature reflects this prioritization; most citations are from security conferences and workshops, followed closely by leading human-computer interaction conferences and workshops. Literature was found and pulled through IEEE Xplore, ACM Digital Library, SpringerLink, and Onesearch databases. Our search included a particular focus on top security conferences and workshops such as USENIX Security Symposium, IEEE Symposium on Security and Privacy, and Symposium on Usable Privacy and Security. To include human systems research, the selection also comprises usable security papers from the Conference on Human Factors in Computing Systems and Human Computer Interaction International. As of early 2022, this survey was accurate based on access time. Due to the breadth of research in Usable Security and Privacy, this is not a comprehensive review of these topics; but, through the content provided, shows the common themes, trends, and challenges of the field.

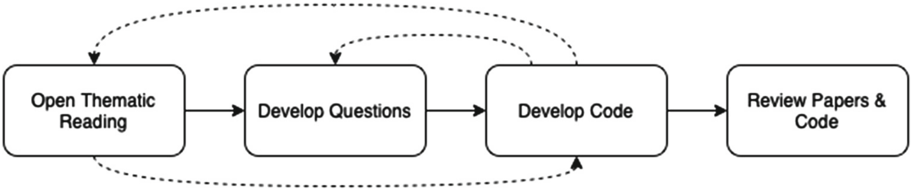

Fig. 1. Flow diagram of the methods and approach taken in this survey paper. The dashed lines indicate a repeated process, while the solid lines indicate the main process flow.

This paper seeks to apply qualitative meta-data analysis techniques to survey usable security and privacy work. For this approach the team used QSR International's Nvivo Software [29]. We followed the electric coding methods discussed by Saldaña that allows multiple methods [46]. Figure 1 details the process that was followed in this user-focused survey. Documents were collected based on the inclusion criteria. Then, open thematic reading of literature generated common themes. The open reading, focused on user-centered security studies, resulted in detecting trends, user perception, and challenges remaining in the field. Some of the challenges identified are directly discussed in the citations. At the same time, other challenges became apparent by the lack of inclusion in the sources. Themes found in initial readings provided content that spurred questions this survey seeks to investigate further. After developing the questions for this survey, we developed a codebook to answer the questions. Open coding ensured we captured any additional themes or findings. Coding is an iterative process, with re-reading, updating, and reviewing. Figure 1 captures this by including dotted lines between steps that occurred multiple times. Finally, we are left with a qualitatively led process to answer the user-centered questions (Table 1).

Table 1. Table of 47 publications analyzed

No.	Reference
1	Acquisti et al. (2017) [1]
2	Benenson et al. (2015) [3]
3	Bilogrevic et al. (2021) [4]
4	Bravo-Lillo et al. (2011) [5]
5	Bravo-lillo et al. (2013) [6]
6	Chassidim et al. (2020) [7]
7	Chin et al. (2012) [8]
8	Consolvo et al. (2021) [9]
9	Downs et al. (2006) [10]
10	Egelman, S. & Peer, E (2015) [12]
11	Egelman et al. (2008) [11]
12	Emami-Naeini et al. (2020) [13]
13	Emami-Naeini et al. (2019) [14]
14	Forget et al. (2019) [16]
15	Frik et al. (2019) [17]
16	Halevi et al. (2013) [19]
17	Haney et al. (2021) [20]
18	Ion et al. (2015) [21]
19	Komanduri et al. (2011) [24]
20	Kondracki et al. (2020) [25]
21	Krombholz et al. (2019) [26]
22	Lebeck et al. (2018) [27]
23	Lennartsson et al. (2021) [28]
24	Mayer et al. (2021) [30]
25	McDonald et al. (2021) [31]
26	Mendel (2019) [32]
27	Naqvi et al. (2019) [34]
28	Pearman et al. (2019) [36]
29	Rader et al. (2012) [37]
30	Ray et al. (2021) [38]
31	Rebensky et al. (2021) [39]
32	Redmiles, E.M. (2019) [40]
33	Redmiles et al. (2018) [44]
34	Redmiles et al. (2019) [41]
35	Redmiles et al. (2016) [42]

(*continued*)

Table 1. (*continued*)

No.	Reference
36	Redmiles et al. (2020) [43]
37	Reeder et al. (2018) [45]
38	Schufrin et al. (2020) [47]
39	Shen et al. (2021) [48]
40	Sheng et al. (2010) [49]
41	Simko et al. (2018) [50]
42	Sunshine(2009) [53]
43	Venkatadri et al. (2018) [54]
44	Wash, R. & Rader, E. (2015) [55]
45	Whitten, A. & Tygar, J.D. (1999) [56]
46	Wu et al. (2018) [57]
47	Zeng et al. (2017) [58]

4 Limitations

Our study encounters sample size issues and methodological limitations when analyzing literature using qualitative meta-analysis. First, the sample size of the literature could be more exhaustive. We selected based on inclusion in security and privacy conferences or human-computer interaction conferences, but this alone can yield more papers. Papers in the survey also needed to include emphasis on non-expert users. To ensure that our sample size was adequate for the analysis of user interactions, we coded to saturation [46]. Using the open code approach, we reached a point where several new articles yielded no more codes for our focus area of user experience.

A best practice for developing qualitative codes is to utilize multiple researchers. First, multiple researchers help to ensure agreement and validity of the codebook. Then, the agreement is evaluated using statistics, such as kappa coefficient [46]. This was not possible for this study, but our analysis can assure validity because the codebook reached saturation.

Finally, another limitation to this survey focusing on user perceptions, interactions, and experience within the privacy and security field, is the divergence between a citations' age and current trends in the area. We hypothesize that changes in user technological expertise, increased reliance on online activities during COVID-19, and other population trends could lead to older publications with results that may no longer be as accurate. For example, a finding in one of the evaluated papers could indicate that the median population sampled does not use 2-Factor Authentication (2FA). If the users were sampled today, we may find that more recent events, such as increase in remote work, have cause greater 2FA adoption.

5 Results

We analyzed a total of 47 papers taken from both the security and privacy domain and human-computer interaction discipline. Documents were found by an extensive search and determined acceptable for inclusion if they (1) discussed security and privacy-related research for non-expert users (2) came from a conference or publication identified for inclusion. After collecting a sizeable pile of material to analyze, we followed the steps outlined in Fig. 1. One researcher read documents to develop initial questions. She returned to the first article and started an open coding process when this was complete. If a theme occurred multiple times, it became part of the codebook. The goal was to find consistent themes across all the documents in several areas: user experience, trends, and challenges. This included more initial codes such as demographics, discussion of ethics, hypotheses, qualitative coding, methods, tools, and technology. A second read-through narrowed the code structure; iterative reading brought some distinctions in results that impacted the code structure. For instance, it became apparent that the trends fit into two main categories: Technology and Methods. Similarly, our hope to identify challenges and new directions lead to two separate code classifications: Challenges and Future Work. We can better determine what challenges remain without recommendations for future work in separating the two. The remaining content of this section focuses on the codebook and data obtained in the qualitative analysis.

5.1 User Experience

One of the questions we sought to answer focused on user risk. First, we wanted to understand better how user risk is framed across technology and demographics. For example, what user-oriented themes surface across all publications surveyed regardless of technology, age, gender, or demographic-specific challenges? Understanding this can help answer the questions around user behavior and beliefs that impact risk. Our qualitative approach provides an answer by identifying themes that reflect user experience. In the open-coding, we developed a code structure shown in Table 2. Misconception is a common theme in 20 of the publications. Surprisingly, Habituation and Personality appeared to be the least common. Trade-offs, which we expected to be widely shared only appeared in 8 of the publications. To demonstrate the frequency of themes, Table 2 includes the paper count for each topic in descending order.

5.2 Trends

We focused on discovering trends through qualitative analysis. User Experiments, Surveys, and Mental Models wove through the existing literature, tie the works together. As a result, Methods became a shared theme. Table 3 lists the methods we recorded in the qualitative analysis. In reading, we saw papers look at various topics, including Chrome alerts, Secure-Socket Layer (SSL) warnings, and Password Managers. We sub-coded Technology and Tools to capture what exactly studies reported. Table 3 lists the technology and tools that were common across the survey analysis.

5.3 Future Work and Challenges

The codes for challenges are listed in Table 4. Future work required adjustment; the themes still are broad enough to have multiple papers assigned to the code but more detailed to sufficiently represent the content discussed. The themes around challenges and future work were separated for analysis. During the open coding process, many of the difficulties identified mapped to specific items as future work. Figure 2 shows how the challenges mapped to specific future work themes reported. In this figure, we tried to reflect the relationship between two themes by color. Themes that did not have an item in the other column are gray to indicate no relationship. If we take one of the future work items, for example, Assist Users with Defaults, we see many challenges it addresses. In this example, adding defaults can help habituation by avoiding overexposing users to warnings. Similarly, the concept of designing smart user defaults is a part of improving user interface design and access control mechanisms. Interdependencies and the rapid change of technology are two challenges mentioned by more than one publication but are not addressed in the themes that emerged around future work. We find some future work that, while important, does not reflect the most common challenges reported in our survey.

Table 2. Themes found in the user-centered analysis along with count of papers that reported on theme

Themes	Publication count
Misconceptions	20
Tool Improvements	14
Trust	13
Knowledge & Skill	12
Timeliness	10
Advice	9
Trade-off	8
Security and Privacy Settings	7
Threats	7
Lack of Information	5
Dependency	5
Data Collection	5
Habituation	5
Personality	2

Table 3. The trends found in methods and technology application across the 47 papers surveyed

Methods
Experiment
Interview
Literature Survey
Mental Model
Modes and Frameworks
Survey
Themes

Technology and Tools
Browsers
Mobile device
Phishing attacks
Messages and Warnings
IoT
Labels
Social Media
Passwords
HTTPS
Augmented Reality
Data
Password Managers
Authentication

Table 4. The trends found in challenges and future work across the 47 papers surveyed

Challenges
One-Size Fits All
Habituation
Trade-off
Rapid Change of Technology
Knowledge & Skill
Inform
User Interface Design
Access Control
Misconceptions
Ecosystem Inter-Dependencies
Data Format and Storage
Unknowns for Certain Demographics

Future Work
Assist Users with Defaults
Mental Models
Understand Trade-offs
Design Warnings to Inform
Communicate Data Collection
Improve Security Education
Examine from New Perspectives
More Analysis of 2FA Adoption
Legal Actions
Standardize Interfaces
Better Measurements

6 Discussion

We have so far presented results that follow immediately from our data. In this section, we will answer the two research questions based on the findings of this survey and discuss key discoveries from the results of the qualitative analysis.

6.1 RQ1 [User Experience and Risk]: *What User Behaviors put Users More at Risk, and What Do Users Believe Places them Most at Risk?*

There is a relationship between risky behaviors, users' beliefs, and misconceptions. Our results indicate that the risky behaviors, beliefs, and misconceptions

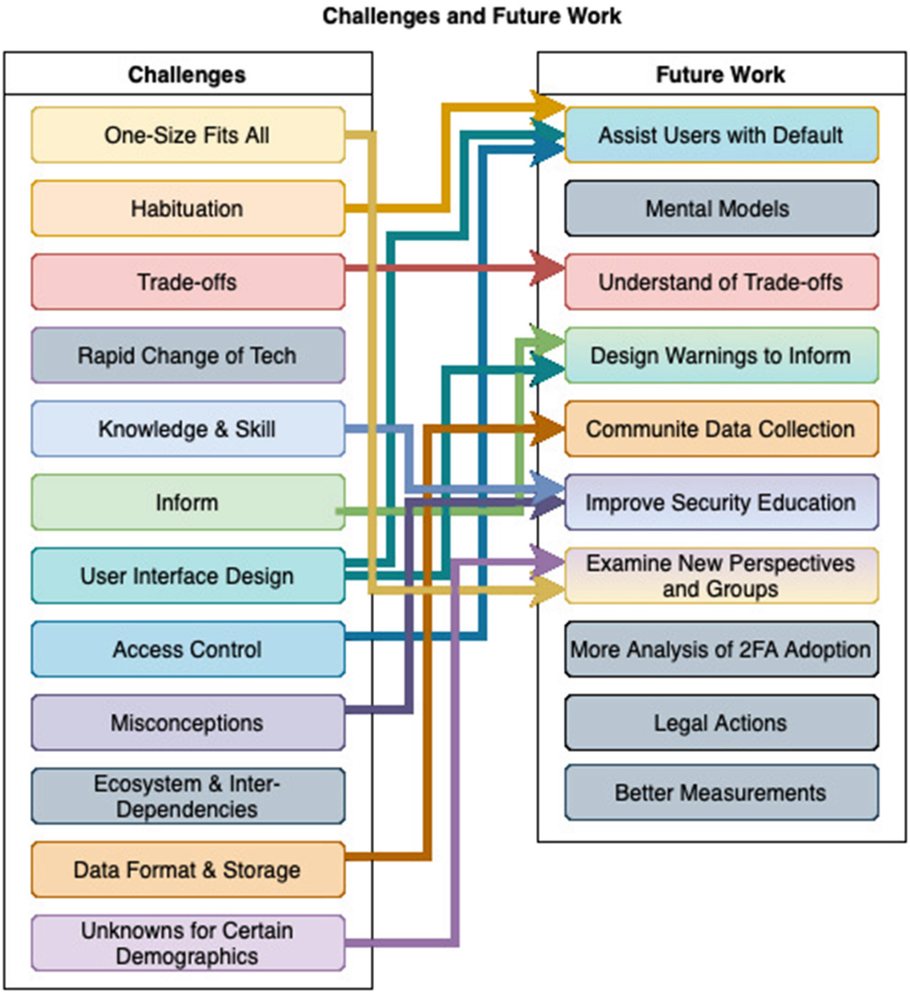
Challenges and Future Work
Challenges
One-Size Fits All
Habituation
Trade-offs
Rapid Change of Tech
Knowledge & Skill
Inform
User Interface Design
Access Control
Misconceptions
Ecosystem & Inter-Dependencies
Data Format & Storage
Unknowns for Certain Demographics
Future Work
Assist Users with Default
Mental Models
Understand of Trade-offs
Design Warnings to Inform
Communite Data Collection
Improve Security Education
Examine New Perspectives and Groups
More Analysis of 2FA Adoption
Legal Actions
Better Measurements

Fig. 2. Relationship between common challenges and commonly identified future work in the surveyed publications

are integral to the user experience. Our analysis found that the motivation for risky behaviors stemmed from misconceptions, lack of knowledge, or design flaws. Users engage in risky behaviors when the security and privacy solutions are not friendly. This was especially true for password management. Pearman et al. found that people who do not use password management tools "indicated multiple risky password habits, including heavy reuse of passwords and few or no unique passwords" [36]. Permissions, access control, and settings seemed to be a continuous challenge for users. Many users did not make changes when the interface did not work intuitively or provide users with the most secure options. Shen et al. reported on this relationship: "Users may notice unexpected permissions after reviewing their permission settings yet few of them (two out of 20) regularly review their permission settings" [48]. Reviewing permissions requires users to be active and mindful of settings. Even if users find unwanted settings, they rarely seek to change things.

In fact, according to the literature surveyed, it may be best to remove users' need to act when it comes to security-related decisions. Offering security and privacy features as defaults can avoid dangerous actions. Forget et al. and Sunshine et al. conducted two different investigations. Still, both found that users tend to make risky decisions, and removing security maintenance from the user can offer better protection. The thematic analysis by Forget et al. suggests that users who did not actively manage settings by resorting to defaults were more secure [16].

Similarly, in looking at warnings, Sunshine et al. and Bravo-Lillo et al. found that removing users' interactions with warnings and, instead, providing filtering methods to protect the user would increase security [5,53]. Users need assistance to avoid risky decisions. Poor decisions occur due to a lack of urgency and an incorrect understanding. When examining user response to unauthorized account access, Redmiles found that users were slow to act [40].

In the same publication, user beliefs factored into the response, "Collectivist cultural identity appears to influence both participants' threat models and support sources. Participants from more collectivistic cultures (Vietnam, Brazil, and India) were more concerned about someone they knew gaining access to their account than an unknown 'hacker'" [40]. End users develop models of threats, and these models influence their reaction. When users have misconceptions of the model, they take riskier actions. Wash et al. report on this: "Many participants reported weakly held beliefs about viruses and hackers, and these were the least likely to say they take protective actions" [55]. This often comes from a lack of knowledge or understanding of the technology. Many of the citations surveyed here report how users make risky decisions when they do not completely understand the meaning of warnings. For example, in the case of website security, Downs et al. found that "most participants had seen lock images on a web site, and knew that this was meant to signify security, although most had only a limited understanding of what that meant or how to interpret" [10]. Understanding what a user interface is communicating can help users create a more accurate understanding of what is risky and what is not risky.

Recent research exploring different populations and user groups has found design and mental models critical for users to make secure decisions and avoid unnecessary risk. In this survey, we found publications that looked at three distinct user groups: older adults [17,38], refugees [50], and sex workers [31]. These unique groups had increased dependencies on technology that could increase risks to the user. For example, the adults in care facilities often become dependent on the technology to ensure safety. A participant in Frik et al.'s study summarizes this, "'You cede a lot of your personal privacy rights when you move into a place like this, in exchange for services being rendered to you"' [17]. Older adults encounter other dependencies that increase risks, such as dependencies on family or limited resources. In the literature surveyed we found that older adults rely on close individuals to help with security settings. In some cases, we also find that older adults are more limited in resources and rely more on recycled devices or public computers. All these actions put increased risk on privacy and security [17].

Refugees experience similar, if not at times more polarizing, dependencies. For example, refugees are often dependent on their case manager [50]. Another issue facing refugees is that technology solutions to provide security do not consider challenges for this user group. Simko et al. provide the example of password questions. Password questions do not accurately reflect experiences that refugees can relate and, therefore, answer [50]. Sex workers face similar limitations with technology that can force them to make riskier decisions by avoiding secure payment options [31]. In the cited work, sex workers report understand the risks and opt to avoid using the technology due to the limitations.

User behaviors are, in a way, responses to nudges and cues. Acquisti et al. argue that importance of understanding nudges in decision-making can help to provide avenues for safer security and privacy [1]. From our survey, we find that the risky behaviors users take result from poor user interfaces and incomplete understandings of security. With misconceptions and insufficient nudges, users will be inclined to move toward decisions that increase risk. Whether users are aware of the risks, security and privacy measures should be available and designed for all user groups. Without inclusive design, those most at risk of threats will be unprotected.

6.2 RQ2 [Trends and Challenges]: *What are Emerging Trends and Challenges to the Field?*

Trends. Interviews, surveys, and experiments were the most common methods in the publications analyzed. Our coding found 17 publications used interviews, 21 used surveys, and 18 used experiments. These methods are essential for collecting user information. In an analysis of user responses, Redmiles et al. found that survey data and measurements of users do not always match; however, reporting bias can be improved through filtering and weighting survey data [41]. These methods are tried and true across various fields and are likely to continue being heavily relied upon in the usable security and privacy space. Table 3 lists the themes that emerged for methods during this survey.

Table 3 also includes the results for technology and tools. Warnings and phishing are some of the best-studied areas [6,10,11,16,45,53,57]. However, we see emerging technology becoming more prominent. Emerging technology publications in this review included IoT and Augmented Reality [13,14,20,27,58]. Among other notable trends is a renewed focus on at-risk users. Since demographics is not a tool or technology, it was not captured as a theme in Table 3, but the increase in research is apparent. Our analysis found recent reports looked at specific demographics, such as older adults or refugees. This suggests a growing interest in the research community to better understand diverse users.

Challenges and Future Work. We examined challenges and future work through thematic analysis. Despite nearly 40 years of research, usable security and privacy still faces obstacles. Many of the impediments can be summarized by usability or user awareness. In our analysis of thematic codes, we found areas that were identified for future research or categories that represent unaddressed challenges. For example, security settings may not transfer between devices in modern IoT ecosystems. Users must learn new interfaces and constantly update settings for every new device. The lack of standardization is a challenge that more than one publication discussed. However, none of the items under future work in Fig. 2 reflect this gap. Future work identifies other areas that need development, even if the corresponding challenge did not emerge in the open coding process. We highlight obvious gaps and remaining work in the field here through the themes identified in Fig. 2.

One remaining challenge that became apparent in the survey is the limitation of data. Some authors reported limitations around measurements; better measurements mean researchers can sufficiently capture user experience [44]. After reading through the publications presented here, we expand upon the need to have more data and measurements. Trends and well-established challenges implore researchers to continue toward inclusive design, but gaps remain.

Currently, we can evaluate mental models, technology, user interface (UI) designs, but the research community lacks an understanding of how users have changed over time. We expect to see changes in users; we hypothesize that this change can be due to increased technology adoption and improved usable security and privacy. Some of the studies in this paper are nearly 20 years old, while others are recent. In this survey, it became apparent that there are limits on measuring how users' risks have evolved. We can look at how the research trends have changed over time, but this speaks more to what the research community is focusing on rather than what changes users are experiencing. Table 2 shows the challenges and remaining work identified in the publications examined. After analyzing the trends and challenges, we believe there is also a need to expand user data collection for usable security and privacy and possible metrics to evaluate the data. In future work, our team hopes to investigate this specific challenge. Data can enable us to answer questions about user experience over time or after a significant event, like COVID-19.

7 Conclusion

So much work in usable privacy and security focuses on technology and application. Our goal is to step outside the application and away from expert users to help generalize findings for novice users. Through reading and qualitative analysis, we find that there are many shared methods, trends, and challenges among the surveyed publications. This paper delivers a systematic literature survey of user experience and remaining work. We demonstrate common themes reported in the 47 publications and we devise risky behaviors common to non-experts. Our survey paper dives into the remaining gaps identified in current work and extrapolates other challenges. By presenting generalizable end-user-specific themes, we portray similarities between existing work. We have an opportunity to build upon existing work, emerging trends, and remaining questions in the field to better incorporate users in the design and development of privacy and security features.

References

1. Acquisti, A., et al.: Nudges for privacy and security. ACM Comput. Surv. **50**(3), 1–41 (2017). https://doi.org/10.1145/3054926
2. Albanese, M., et al.: Computer-aided human centric cyber situation awareness. In: Liu, P., Jajodia, S., Wang, C. (eds.) Theory and Models for Cyber Situation Awareness. LNCS, vol. 10030, pp. 3–25. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61152-5_1
3. Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., Uebelacker, S.: Maybe poor Johnny really cannot encrypt. In: Proceedings of the 2015 New Security Paradigms Workshop, pp. 85–99. ACM, New York, September 2015. https://doi.org/10.1145/2841113.2841120. https://dl.acm.org/doi/10.1145/2841113.2841120
4. Bilogrevic, I., et al.: "Shhh... be quiet!" reducing the unwanted interruptions of notification permission prompts on chrome. In: USENIX Security Symposium (2021)
5. Bravo-Lillo, C., Cranor, L.F., Komanduri, S.: Bridging the gap in computer security warnings: a mental model approach. IEEE Secur. Priv. **9**, 18–26 (2011)
6. Bravo-lillo, C., Cranor, L.F., Downs, J., Reeder, R.W., Schechter, S.: Your attention please designing security-decision UIs to make genuine risks harder to ignore. In: Symposium On Usable Privacy and Security (2013). https://www.microsoft.com/en-us/research/publication/your-attention-please-designing-security-decision-uis-to-make-genuine-risks-harder-to-ignore/
7. Chassidim, H., Perentis, C., Toch, E., Lepri, B.: Between privacy and security: the factors that drive intentions to use cyber-security applications. Behav. Inf. Technol. **40**(16), 1769–1783 (2020). https://doi.org/10.1080/0144929X.2020.1781259
8. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: Proceedings of the 8th Symposium on Usable Privacy and Security, SOUPS 2012, p. 1. ACM Press, New York (2012). https://doi.org/10.1145/2335356.2335358. http://dl.acm.org/citation.cfm?doid=2335356.2335358
9. Consolvo, S., Kelley, P.G., Matthews, T., Thomas, K., Dunn, L., Bursztein, E.: "Why wouldn't someone think of democracy as a target?": security practices & challenges of people involved with U.S. political campaigns. In: Proceedings of the 30th USENIX Security Symposium, pp. 1181–1198 (2021). https://www.usenix.org/conference/usenixsecurity21/presentation/consolvo
10. Downs, J.S., Holbrook, M.B., Cranor, L.F.: Decision strategies and susceptibility to phishing. In: Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS 2006, vol. 149, p. 79. ACM Press, New York (2006). https://doi.org/10.1145/1143120.1143131
11. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Conference on Human Factors in Computing Systems - Proceedings, pp. 1065–1074. ACM Press, New York (2008). https://doi.org/10.1145/1357054.1357219. http://portal.acm.org/citation.cfm?doid=1357054.1357219

12. Egelman, S., Peer, E.: Predicting privacy and security attitudes. ACM SIGCAS Comput. Soc. **45**(1), 22–28 (2015). https://doi.org/10.1145/2738210.2738215. https://dl.acm.org/doi/10.1145/2738210.2738215
13. Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., Hibshi, H.: Ask the experts: what should be on an IoT privacy and security label? In: Proceedings - IEEE Symposium on Security and Privacy 2020-May, pp. 447–464 (2020). https://doi.org/10.1109/SP40000.2020.00043
14. Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F.: Exploring how privacy and security factor into IoT device purchase behavior. In: Conference on Human Factors in Computing Systems - Proceedings, pp. 1–12 (2019). https://doi.org/10.1145/3290605.3300764
15. Es-Salhi, K., Espes, D., Cuppens, N.: RIICS: risk based IICS segmentation method. In: Zemmari, A., Mosbah, M., Cuppens-Boulahia, N., Cuppens, F. (eds.) CRiSIS 2018. LNCS, vol. 11391, pp. 143–157. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12143-3_13
16. Forget, A., et al.: Do or do not, there is no try: user engagement may not improve security outcomes. In: 12th Symposium on Usable Privacy and Security, SOUPS 2016, pp. 97–111 (2019). https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget
17. Frik, A., Nurgalieva, L., Bernd, J., Lee, J.S., Schaub, F., Egelman, S.: Privacy and security threat models and mitigation strategies of older adults. In: Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019, pp. 21–40 (2019)
18. Gove, R.: Automatic narrative summarization for visualizing cyber security logs and incident reports. IEEE Trans. Vis. Comput. Graph. **28**(1), 1182–1190 (2022). https://doi.org/10.1109/TVCG.2021.3114843
19. Halevi, T., Lewis, J., Memon, N.: A pilot study of cyber security and privacy related behavior and personality traits. In: Proceedings of the 22nd International Conference on World Wide Web - WWW 2013 Companion, pp. 737–744. ACM Press, New York (2013). https://doi.org/10.1145/2487788.2488034. http://dl.acm.org/citation.cfm?doid=2487788.2488034
20. Haney, J., Acar, Y., Furman, S.: “It’s the company, the government, You and I”: user perceptions of responsibility for smart home privacy and security. In: 30th Security Symposium (Security 21) (2021)
21. Ion, I., Reeder, R., Consolvo, S.: “...No one can hack my mind”: comparing expert and non-expert security practices. In: Proceedings of the 11th Symposium on Usable Privacy and Security, SOUPS 2015, pp. 327–346 (2015)
22. Karat, C.M.: Iterative usability testing of a security application. Proc. Hum. Factors Soc. Annual Meeting **33**(5), 273–277 (1989). https://doi.org/10.1177/154193128903300508
23. Kokulu, F.B., et al.: Matched and mismatched SOCs: a qualitative study on security operations center issues. In: Proceedings of the ACM Conference on Computer and Communications Security, pp. 1955–1970 (2019). https://doi.org/10.1145/3319535.3354239
24. Komanduri, S., et al.: Of passwords and people: measuring the effect of password-composition policies. In: Conference on Human Factors in Computing Systems - Proceedings, pp. 2595–2604. ACM, New York, May 2011. https://doi.org/10.1145/1978942.1979321. https://dl.acm.org/doi/10.1145/1978942.1979321
25. Kondracki, B., Aliyeva, A., Egele, M., Polakis, J., Nikiforakis, N.: Meddling middlemen: empirical analysis of the risks of data-saving mobile browsers. In: Proceed-

ings - IEEE Symposium on Security and Privacy 2020-May, pp. 810–824 (2020). https://doi.org/10.1109/SP40000.2020.00077

26. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., von Zezschwitz, E.: "If HTTPS were secure, I wouldn't need 2FA" - end user and administrator mental models of HTTPS. In: 2019 IEEE Symposium on Security and Privacy (SP), vol. 2019-May, pp. 246–263. IEEE, May 2019. https://doi.org/10.1109/SP.2019.00060. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835228
27. Lebeck, K., Ruth, K., Kohno, T., Roesner, F.: Towards security and privacy for multi-user augmented reality: foundations with end users. In: Proceedings - IEEE Symposium on Security and Privacy 2018-May, pp. 392–408 (2018). https://doi.org/10.1109/SP.2018.00051
28. Lennartsson, M., Kävrestad, J., Nohlberg, M.: Exploring the meaning of usable security - a literature review, October 2021. https://doi.org/10.1108/ICS-10-2020-0167
29. QIP Ltd.: Nvivo (2020). https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home
30. Mayer, P., Kastel, S., Zou, Y., Schaub, F., Aviv, A.J.: "Now I'm a bit angry:" individuals' awareness, perception, and responses to data breaches that affected them. In: USENIX (2021)
31. McDonald, A., Barwulor, C., Mazurek, M.L., Schaub, F., Redmiles, E.M.: "It's stressful having all these phones": investigating sex workers' safety goals, risks, and practices online. In: Proceedings of the 30th USENIX Security Symposium, pp. 375–392 (2021)
32. Mendel, T., Toch, E.: My Mom was getting this popup. Proc. ACM Interact. Mob. Wearable Ubiquit. Technol. **3**(4), 1–20 (2019). https://doi.org/10.1145/3369821. https://dl.acm.org/doi/10.1145/3369821
33. Naidoo, R.: A multi-level influence model of COVID-19 themed cybercrime. Eur. J. Inf. Syst. **29**(3), 306–321 (2020)
34. Naqvi, B., Seffah, A.: Interdependencies, conflicts and trade-offs between security and usability: why and how should we engineer them? In: Moallem, A. (ed.) HCII 2019. LNCS, vol. 11594, pp. 314–324. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22351-9_21
35. Nyre-Yu, M., Sprehn, K.A., Caldwell, B.S.: Informing hybrid system design in cyber security incident response. In: Moallem, A. (ed.) HCII 2019. LNCS, vol. 11594, pp. 325–338. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22351-9_22
36. Pearman, S., Zhang, S.A., Bauer, L., Christin, N., Cranor, L.F.: Why people (don't) use password managers effectively. In: Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019, pp. 319–338 (2019). https://www.usenix.org/conference/soups2019/presentation/pearman
37. Rader, E., Wash, R., Brooks, B.: Stories as informal lessons about security. In: Proceedings of the 8th Symposium on Usable Privacy and Security, SOUPS 2012, p. 1. ACM Press, New York (2012). https://doi.org/10.1145/2335356.2335364. http://dl.acm.org/citation.cfm?doid=2335356.2335364
38. Ray, H., Wolf, F., Kuber, R., Aviv, A.J.: Why older adults (don't) use password managers. In: Proceedings of the 30th USENIX Security Symposium, pp. 73–90, 2021. www.usenix.org/conference/usenixsecurity21/presentation/ray
39. Rebensky, S., Carroll, M., Nakushian, A., Chaparro, M., Prior, T.: Understanding the last line of defense: human response to cybersecurity events. In: Moallem, A. (ed.) HCII 2021. LNCS, vol. 12788, pp. 353–366. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77392-2_23

40. Redmiles, E.M.: ‘Should i worry?’ A cross-cultural examination of account security incident response. In: Proceedings - IEEE Symposium on Security and Privacy, vol. 2019-May, pp. 920–934 (2019). https://doi.org/10.1109/SP.2019.00059
41. Redmiles, E.M., Kross, S., Mazurek, M.L.: How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. In: Proceedings - IEEE Symposium on Security and Privacy, vol. 2019-May, pp. 1326–1343 (2019). https://doi.org/10.1109/SP.2019.00014. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8835345
42. Redmiles, E.M., Malone, A.R., Mazurek, M.L.: I think they’re trying to tell me something: advice sources and selection for digital security. In: Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, pp. 272–288 (2016). https://doi.org/10.1109/SP.2016.24
43. Redmiles, E.M., et al.: A comprehensive quality evaluation of security and privacy advice on the web. In: Proceedings of the 29th USENIX Security Symposium, pp. 89–108 (2020)
44. Redmiles, E.M., Zhu, Z., Kross, S., Kuchhal, D., Dumitras, T., Mazurek, M.L.: Asking for a friend: evaluating response biases in security user studies. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1238–1255. ACM, New York, October 2018. https://doi.org/10.1145/3243734.3243740
45. Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., Egelman, S.: An experience sampling study of user reactions to browser warnings in the field. In: Conference on Human Factors in Computing Systems - Proceedings, vol. 2018-April, pp. 1–13. ACM, New York, April 2018. https://doi.org/10.1145/3173574.3174086
46. Saldaña, J.: The Coding Manual for Qualitative Researchers. Sage (2009)
47. Schufrin, M., Reynolds, S.L., Kuijper, A., Kohlhammer, J.: A visualization interface to improve the transparency of collected personal data on the internet. In: 2020 IEEE Symposium on Visualization for Cyber Security, VizSec 2020, pp. 1–10 (2020). https://doi.org/10.1109/VizSec51108.2020.00007. https://transparency-vis.vx.igd.fraunhofer.de/
48. Shen, B., et al.: Can Systems Explain Permissions Better? Understanding Users’ Misperceptions under Smartphone Runtime Permission Model. Security (2021)
49. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J.: Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, vol. 1, p. 373. ACM Press, New York (2010). https://doi.org/10.1145/1753326.1753383. http://portal.acm.org/citation.cfm?doid=1753326.1753383
50. Simko, L., Lerner, A., Ibtasam, S., Roesner, F., Kohno, T.: Computer security and privacy for refugees in the United States. In: 2018 IEEE Symposium on Security and Privacy (SP), vol. 2018-May, pp. 409–423. IEEE, May 2018. https://doi.org/10.1109/SP.2018.00023. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418616. https://ieeexplore.ieee.org/document/8418616/
51. National Institute of Standards and Technology: Usable Security & Privacy—NIST. https://www.nist.gov/programs-projects/usable-security-privacy
52. Stevens, R., Votipka, D., Redmiles, E.M., Mazurek, M.L., Ahern, C., Sweeney, P.: The battle for New York: a case study of applied digital threat modeling at the enterprise level. In: Proceedings of the 27th USENIX Security Symposium, pp. 621–637 (2018). https://www.usenix.org/conference/usenixsecurity18/presentation/stevens

53. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., Cranor, L.F.: Crying wolf: an empirical study of SSL warning effectiveness. In: Proceedings of the 18th USENIX Security Symposium, pp. 399–416 (2009)
54. Venkatadri, G., et al.: Privacy risks with Facebook's PII-based targeting: auditing a data broker's advertising interface. In: Proceedings - IEEE Symposium on Security and Privacy 2018-May, pp. 89–107 (2018). https://doi.org/10.1109/SP.2018.00014
55. Wash, R., Rader, E.: Too much knowledge? Security beliefs and protective behaviors among United States internet users. In: Proceedings of the 11th Symposium on Usable Privacy and Security, SOUPS 2015, pp. 309–325 (2015)
56. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: 8th USENIX Security Symposium (1999)
57. Wu, Y., Gupta, P., Wei, M., Acar, Y., Fahl, S., Ur, B.: Your secrets are safe: how browsers' explanations impact misconceptions about private browsing mode. In: The Web Conference 2018 - Proceedings of the World Wide Web Conference, WWW 2018, pp. 217–226 (2018). https://doi.org/10.1145/3178876.3186088
58. Zeng, E., Mare, S., Roesner, F.: End user security & privacy concerns with smart homes. In: Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017, pp. 65–80 (2017). https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng