SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors

Miranda Wei, *University of Washington;* Jaron Mink, *University of Illinois at Urbana-Champaign;* Yael Eiger and Tadayoshi Kohno, *University of Washington;* Elissa M. Redmiles, *Georgetown University;* Franziska Roesner, *University of Washington*

https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-solk

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors

Miranda Wei
University of Washington

Jaron Mink
University of Illinois at Urbana-Champaign

Yael Eiger
University of Washington

Tadayoshi Kohno
University of Washington

Elissa M. Redmiles
Georgetown University

Franziska Roesner
University of Washington

Abstract

Researchers are increasingly exploring how gender, culture, and other sociodemographic factors correlate with user computer security and privacy behaviors. To more holistically understand relationships between these factors and behaviors, we make two contributions. First, we broadly survey existing scholarship on sociodemographics and secure behavior (151 papers) before conducting a focused literature review of 47 papers to synthesize what is currently known and identify open questions for future research. Second, by incorporating contemporary social and critical theories, we establish guidelines for future studies of sociodemographic factors and security behaviors that address how to overcome common pitfalls. We present a case study to demonstrate our guidelines in action, at-scale, that conduct a measurement study of the relationships between sociodemographics and de-identified, aggregated log data of security and privacy behaviors among 16,829 users on Facebook across 16 countries. Through these contributions, we position our work as a systemization of a *lack* of knowledge (SoLK). Overall, we find contradictory results and vast unknowns about how identity shapes security behavior. Through our guidelines and discussion, we chart new directions to more deeply examine how and why sociodemographic factors affect security behaviors.

1 Introduction

Sociodemographic factors — people's social, cultural, or demographic attributes (e.g., gender, race, socioeconomic status, age, or internet skill) — shape their lived experiences, i.e., what happens in their lives, how they are impacted by what happens, and how they make decisions. Prior works find that sociodemographics *do* impact computer security behaviors, e.g., that women may choose weaker passwords than men [62] or that older users choose stronger passwords [3]. These findings suggest that gender and age influence password selection and thereby computer security, potentially motivating interventions that target the underlying causal mechanisms.

The field of computer security has considered the role of the human for decades, e.g., Saltzer and Schroeder's recognition of the importance of psychological acceptability of security solutions in the 1970s [91], and Whitten and Tygar's foundational 1999 paper catalyzed the formation of the field of *usable security* [120]. Focus on the role of sociodemographic factors in computer security behaviors is, however, comparatively new [84]. Given the potential impact of these factors, it is vital to examine the current state of knowledge with respect to sociodemographics and computer security behaviors.[1] With this understanding, it becomes possible to focus future efforts on addressing knowledge gaps and, ultimately, to help improve computer security for everyone.

Our first two research goals are:

- **Goal 1.** Collect and synthesize current knowledge about the quantitative relationship between sociodemographic factors and computer security behaviors.
- **Goal 2.** Enumerate existing knowledge gaps about sociodemographics and computer security behaviors.

Through a focused literature review of 47 papers in selected technical security conferences and a high-level survey of 151 papers in the wider literature, we synthesize trends, e.g., that people of different genders may focus on different security behaviors, as well as identify open opportunities for future research. We focus on quantitative studies, a primary method researchers use to measure security behaviors in relation to specific sociodemographic factors, like gender. Knowledge gaps exist when pertinent sociodemographic factors are omitted in analyses. For example, in our set of 47 papers between 1999 and 2023, we find that 38 consider (binary) gender whereas only 3 consider income, 5 consider race, and 9 consider Internet skill; none consider non-binary gender. We also observe different levels of depth with respect to how sociodemographic factors are analyzed and how differences by factors (if any) are interpreted.

After reviewing the current state of knowledge sociodemographics and behaviors, we identify our third goal:

- **Goal 3.** Formulate guidelines for future research on so-

[1] For brevity, we use 'security' to consistently refer to security and privacy.

ciodemographic factors and security behaviors.

To demonstrate the use of our guidelines in practice and at-scale, we apply the guidelines to conduct and report the results of a case study. Our measurement study uses de-identified, aggregated log data from Facebook to analyze the relationship between security behaviors on the platform and selected sociodemographic factors. We confirm several trends observed through our literature review, while adding nuance to others. Finally, we critically consider the knowledge gaps illuminated by our investigation — particularly, the lack of understanding about *why* sociodemographic factors and security behaviors might be correlated — and chart directions for future research.

2 Background and Motivation

Demographics uses statistics to study trends in human populations [79, 80]. Sociodemographics encompass demographic factors as well as social factors defined by formal institutions, e.g., governments [97], or informal institutions, e.g., sociocultural norms [109]. Conventional studies of sociodemographic factors are positivist, i.e., asserts that knowledge can be empirically measured and there *exists* a correct measurement that scientists can strive for [73]. In presuming objectivity, conventional demography overlooks the historical and political processes that shaped the categories themselves [40, 103, 109].

Categorization abstracts away richness to allow scientists to focus on selected characteristics. As an inherently reductive activity, categorization renders some research more tractable but may not accurately represent lived realities [5, 39]. By assigning people to static, finite groups, those who shift between groups or exist outside those groups, for example, will be systematically misinterpreted [1, 48, 95]. Further, categorization schemes are typically designed by historically and socially privileged groups in ways that can embed power imbalances [68, 79, 90, 105].

***Critical demography*, as an alternative to conventional demography, incorporates the reflexive study of how categories are socially constructed.** As such, it "necessitates an open discussion and examination of *power* in society. Specifically, critical demography elucidates how power both affects and is impacted by demographic processes and events" [40]. Thus, critical demography offers a theory-driven paradigm to study how people behave, informed by social and political history [40], towards epistemological diversity and addressing inequity [73]. Prior work has applied critical demography approaches to deepen knowledge and practice, e.g., in computing education [69]. We apply a critical demography approach to synthesize prior work on sociodemographic differences in security behaviors, but also to map what is not yet known.

3 Literature Review Methods

What is currently known about how sociodemographics affect behavior, and what gaps remain? To scope to studies of users' actual security or privacy behaviors, we excluded studies of intended behavior, concerns, knowledge, or attitudes. As we were also interested in quantitative studies, we only included works that compared behavior between sociodemographic groups, i.e., we excluded work that investigated only one group within a sociodemographic factor.

3.1 Identifying Relevant Work

To identify potentially relevant studies, we defined unique search queries for selected conferences (see Section 3.2) and used the advanced search features of the ACM DL, IEEE Xplore, and the USENIX databases to search full-length research articles (see Table 1). Since these databases do not contain NDSS papers, we also obtained an NDSS paper archive scraped by other researchers. We wrote a `pypdf` [23] script to extract and search text directly from the PDFs using the search strings shown in Table 1. Two researchers independently reviewed paper titles and abstracts of search results to apply the scoping criteria described above and iteratively resolved disagreements to select the final dataset.

Relevant studies are also published in venues beyond computer science conferences; we used Google Scholar to find popular studies from any venue, including journals of business, information science, social science, or grey literature. We then defined two sets of keyword searches (see Table 1), which yielded over 6 million results, so one researcher reviewed the first 3 pages of search results. Finally, we followed citations from papers in our dataset that referred to relevant work, adding 20 studies not identified through search strings. We set no explicit time boundaries for our dataset.

3.2 Full and Focus Datasets

Our final "full" dataset consisted of 151 works. Most papers were published in academic venues such as conferences or journals, but we also included 4 theses, 3 Pew Research studies, and 1 arXiv paper. The full dataset reflects a growing interest in security behaviors with respect to sociodemographic factors across venues and academic disciplines. Much of the dataset (76 papers) was in information science or social science domains and spanned a wide range of venues, from computing (e.g., *Computers in Human Behavior*) to communications and media (e.g., *New Media & Society*) to marketing and business (e.g., *Journal of Interactive Marketing* and *Journal of Management Information Systems*) to social sciences (e.g., SSRN). Another 20 papers were in computer science publications. The distribution of venues is long-tailed since we had 70 papers each from unique domains. We defined a "focus" set of 47 papers by identifying seven conferences

Table 1: Summary of literature review search methods. We used Google Scholar to write custom **search strings** to identify relevant studies in selected computer science **venues** and **databases** as well as in non-CS venues. For each search, we show the **number of results** and **number of included** studies satisfying our scoping criteria. †We implemented manual keyword searches of PDFs scraped from ndss-symposium.org. *We manually reviewed only the first 3 search result pages.

Venue	Database	Search String	# Results	# Included
FOCUS DATASET: Selected Computer Science Venues				
ACM CHI	ACM DL	In abstract: [security OR privacy] AND [behavior OR habits OR practices] and in body text: [gender OR sex OR age OR technical expertise OR education OR race OR culture OR internet skill]	213	14
IEEE S&P	IEEE Xplore	*same as CHI*	90	2
USENIX Security	USENIX.org	[security OR privacy] AND [behaviors OR habits OR practices]	41	2
SOUPS	ACM DL	*same as CHI*	77	17
ACM CCS	ACM DL	*same as CHI*	508	7
ACM CSCW	ACM DL	*same as CHI*	62	4
NDSS	ndss-symposium.org†	*same as CHI*	62	1
FULL DATASET: Beyond Selected Computer Science Venues				
Various	Google Scholar	[cross cultural OR large scale OR demographic] AND [behaviors] AND [security OR privacy]	270K+*	97
Various	Google Scholar	[password OR authentication OR update software OR secure drop OR phishing emails OR encryption OR WiFi OR anti-virus OR HTTP SSL warnings OR tracker blockers OR information disclosure OR self disclosure OR IoT OR VPN] AND [behaviors].	5.8M+*	11

most likely to include papers of interest: four computer security conferences (IEEE S&P, USENIX Security, CCS, NDSS), two HCI conferences with a tradition of including security and privacy (ACM CHI, ACM CSCW), and one conference at the intersection of HCI and security (SOUPS).

3.3 Qualitative Analysis

We qualitatively analyzed papers in our "full" set by coding behaviors studied (dependent variables) and sociodemographic factors considered (independent variables). For further analysis on our "focus" set, we also coded whether a significant relationship was (or was not) found[2] as well as where the study was conducted, the research methods used, and any research sample limitations.

We created our codebooks via a series of iterative coding sessions between two coders. First, a primary coder prepared an initial codebook by inductively coding all papers. A second coder then independently coded a subset of the papers using the same codebook. The two coders then met to resolve inconsistencies and, if necessary, clarify and adjust the codebook. If adjustments were made, the primary coder then recoded the rest of the dataset. This process was repeated until the codebook no longer changed. We also verified our resulting codebook with a prior work's codebook on security behaviors [89]. Table 2 presents the behaviors codebook and paper counts; codebooks for other topics are presented in Appendix A.1.

[2]Because studies sometimes studied multiple sociodemographic factors for a given behavior, we coded each relationship separately.

3.4 Positionality

The authors' particular social, cultural, political, and historical context influence the way we discuss sociodemographic factors in this work. As researchers who have predominately lived and worked in the U.S., have English as a first language, and have had opportunities to pursue or achieve academic degrees in computer science, our perspective is limited by the privileges these experiences afford, relative to different experiences. Our motivation for this work is also shaped by experiences of marginalization by gender, culture, race, and age. As researchers with substantial experience studying human factors in security, we aim to improve the security of all people, not only those who have been historically prioritized in security research (i.e., users who are predominantly men, white, wealthy, highly educated, and live in the U.S.). We seek to raise the voices of those at the margins, in alignment with standpoint theory's premise that non-dominant social groups contribute critical knowledge towards scholarship and action towards justice [11].

3.5 Limitations

We sought as exhaustive a list of papers as possible to study sociodemographic factors and security behaviors, but we likely missed some relevant papers. During paper collection, we ultimately included less than 25% of our search results because many papers use sociodemographic keywords without satisfying our criteria, i.e., they do not quantitatively compare groups within a factor. Relevant work is also published outside the seven venues of our focus papers, but we believe our

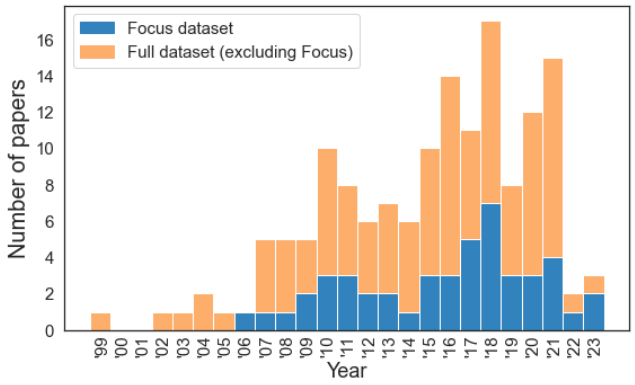

Figure 1: Number of papers in focus and full datasets investigating sociodemographics and security behaviors over time.

methods captured a set of papers large enough for meaningful analysis and discussion.

Our goal was to focus on sociodemographic factors related to security behaviors. As such, we scope to papers that measure security behaviors directly, e.g., through observational data, log data, and self-reports about actual behaviors. Future work may seek to focus on the substantial literature on additional topics, such as attitudes, opinions, or perceptions.

Since our goal was to conduct a formative literature review of security behaviors with respect to sociodemographic factors, we did not attempt to evaluate the "validity" of any paper. The replication crisis in psychology [102] reminds us that robust quantitative findings must be repeatedly tested and confirmed, which we leave to future work.

4 Literature Review Results

We first survey the locations, methods, and behaviors investigated in the full dataset of 151 papers (Section 4.1) and then explore methodological considerations in our 47 focus papers (Section 4.2). Next, we synthesize results about eight sociodemographic factors—gender, age, education, technical expertise, Internet skill, geography, race, and income—from the focus papers (Sections 4.3-4.8). Table 3 provides an overview of sociodemographic factors studied with respect to security behaviors and whether differences among groups were found.

Throughout this section, we enumerate trends as **T#** and opportunities for future work as **O#** to facilitate later comparison with our measurement study results. We present a summary of all trends and opportunities in Table 4.

4.1 Survey of Full Dataset

Since 1999, the publication year of the first study in our dataset, papers on sociodemographics and security have steadily increased (see Figure 1).

Table 2: The number of security behaviors studied by papers in our **full** (N=151) and **focus** (N=47) dataset. Counts do not sum to 151 or 47 due to papers that study multiple behaviors.

Security Behavior	Full	Focus
Network and Web, e.g., VPNs, use private browsing, use anti-tracker tools	44	9
Phishing and Spam, e.g., phishing susceptibility	38	9
Social Sharing, e.g., disclosing info. on social media, changing privacy settings	35	11
Authentication and Accounts, e.g., password creation or reuse, 2FA	23	12
Device, e.g., anti-virus software, mobile lock screens	21	8
Composite: combined security behaviors from above that cannot be disaggregated	14	5

Most studies are conducted in the U.S. or Western Europe O4. A plurality of studies in the full dataset (N=151) were conducted in the U.S. or Western Europe (60), followed by Asia (20), Africa and the Middle East (9), Australia (6), and South America (3).[3] Studies in the focus dataset (N=47) show the same trend: U.S. or Western Europe (33), Asia (5), Africa and the Middle East (3), Australia (3), South America (2).

Studies reflect a significant interest in network and web security behaviors as well as phishing and spam, but comparatively less in other behavior types O14. A complete breakdown of behaviors studied by papers in our full and focus datasets is presented in Table 2. The largest portion of our full dataset investigated network and web-related behaviors (44 papers), such as using VPNs or avoiding public WiFi, or using private browsing and other anti-tracking tools or practices. The second largest portion investigated phishing or spam susceptibility, a much narrower set of behaviors than network and web yet studied by nearly as many studies (38 papers). Less commonly studied were social sharing behaviors, e.g., disclosing information or changing privacy settings on social media (35), authentication and account behaviors (23), and device-related behaviors (21). Finally, 14 papers studied composite security behaviors, or combinations of the above types of behaviors, with regression analyses that we could not disaggregate.

Security behaviors are primarily investigated through self-report methods O15. For our full dataset, the vast majority, i.e., 109 studies, were based on self-reports of security behavior. Less common were the 32 studies that used experimental measurement methods, e.g., in-lab or online experiments, or the 15 that used observational methods, e.g., log data or installed software on user devices. For the focus dataset, 32 were self-reports, 12 used experimental measurement methods, and 8 used observational methods. The significant preference for self-report methods likely reflects the relative convenience of collecting data from participants simply by asking them, but

[3] Counts do not sum to 151 due to studies conducted in multiple locations.

self-reporting may not be wholly accurate given participant biases, e.g., social desirability biases [83]. Future work should confirm these results with more ecologically valid methods.

4.2 Methods Considerations in Focus Dataset

For the focus dataset, we were interested in how prior work ensured that the research was robustly designed and conducted for the sociodemographics and security behaviors of interest.

A sizeable proportion of investigations did not mention sociodemographic factors until the results section of the papers O16. We analyzed focus dataset papers to determine if they motivated their study of sociodemographics in the research questions or introductory section (i.e., considered) or whether sociodemographic factors were mentioned only in the results section (i.e., post hoc). Because clearly defining independent variables, e.g., gender, and their levels or conditions, e.g., woman/man/nonbinary, is essential to control for confounding factors between conditions [81], not considering the role of sociodemographics until the results may imply an incomplete methodology. Further, consistently reporting the variables and relationships of interest before beginning statistical testing is important to avoid cherry-picking non-null results [63]. We found 74 instances where factors were considered in advance and 45 instances where sociodemographic factors were studied post hoc.[4] Studying sociodemographic relationships to security behavior is not warranted merely because relevant data was collected; therefore, confirming the results of papers that conducted a post hoc study of sociodemographics is an opportunity for future research to ensure that the findings were not spurious.

The majority of papers had limited samples, i.e., samples not representative of broader populations or balanced among groups O17. To assess the generalizability of studies in our focus dataset, we coded whether papers were representative (i.e., sample attributes matched broader population attributes), or balanced (i.e., equally across factor groups) for analysis. We found only 7 instances of factors being balanced and 18 representative; the vast majority (96) were limited,[5] i.e., not controlled in any way (snowball or convenience samples), or had no description of recruiting considerations. Future work should expand on addressing limited samples.

4.3 Gender

Gender is used in varying contexts and includes a person's gender, but also how gender is constructed in a societal context, i.e., referring to socially established gender roles [49]. It is often conflated with sex, i.e., bodily attributes, though these are distinct concepts [49]. Gender has received the most attention in security research (38 of 47 focus papers) relative to other sociodemographic factors.

Existing research primarily uses self-report methods, which could be biased by gendered differences in self-reporting O2. Prior work finds gender stereotypes that men are overconfident when it comes to security and privacy [119]. As described above, sociodemographic differences in behavior tend to be investigated through self-report methods, a trend that holds for gender specifically: of 28 papers that found gender differences, 21 used self-report methods. Thus, gender differences could be because men are more likely to self-report behaviors than women, regardless of true adoption rates.

Prior work suggests men may focus more on technical security behaviors, while women may focus more on privacy behaviors T1. One set of papers found that men were more likely to take certain protective actions related to network and web security, e.g., use tracker blockers [60], take protective actions against trackers [13], and use private browsing [29], although no differences were found for heeding SSL warnings [106]. Two papers studied composite security behaviors, finding that men were more likely to adopt predefined sets of security and privacy protective practices [118, 126] (although no differences were found in "triggers" prompting security behaviors [18]). Finally, one paper investigated how the sources for security advice differ between genders [87], finding that men were more likely than women to source advice from service providers. Taken together, these findings suggest gender differences in "technical" security behaviors, though it is unclear whether these differences result from self-reporting biases, prior computing experience, attitudes towards computers [122], or something else.

Another set of papers found that women were more likely to engage in security and privacy behaviors on social media and personal devices. Women were more likely to have private profiles on Facebook or Myspace [27, 107], post non-publicly on Facebook [24] and Snapchat [30], and avoid actions that expose online profiles they viewed [41]. Teen girls were found to be more likely than teen boys to adopt risk-coping behaviors (e.g., deleting posts, untagging photos, faking personal information) as well as seek privacy advice [43]. Prior work also found differences in disclosure content: men were more likely to disclose COVID-19 distress in May 2020 than women [125], but generally women were more likely to share memes portraying subjects positively [34]. Though prior work found inconclusive evidence about gender differences in device behaviors — adopting lock screens [31, 115], Android updating [59] — in others, women were found to be more likely to use webcam covers [56] and women 18-23 were more likely than men or people of other age groups to deny Android permission dialogs [2]. Taken together, these findings align with prior work (outside our literature review) [45, 57, 82, 92, 111] indicating that women focus on information protection and engage in privacy-preserving self-censorship.

[4] Papers would have multiple instances if they studied multiple factors; thus, counts do not sum to 47.

[5] Counts do not sum to 47 because of papers studying multiple factors.

Results were mixed on gender differences with respect to authentication and susceptibility to phishing and spam. Research on authentication behaviors is mixed: two papers found that men's passwords were stronger against offline attacks [3, 62], but men aged 46-49 were more likely to share passwords than others [47]; another paper did not find sharing differences by gender [74]. Further, researchers found that women were more likely to reuse passwords with slight modifications [99], less likely to remember graphical passwords [8], and less likely to enable 2FA in response to experimental prompts [28], but other researchers found no difference in password reuse [78] or in whether they change password managers [66]. Future work should investigate whether gender differences in authentication behaviors are due to methodological differences, context, or other reasons **O8**.

Two papers found that women were more likely to click on phishing and spam [86, 100], although three other papers did not find significant gender differences in this regard [21, 52, 101], and one found that women were less likely to visit malicious URLs than men [98]. Papers not finding gender differences were published in 2006, 2007, and 2009, while papers finding differences were published in 2010 and 2018. One explanation could be that phishing and spam increasingly targeted women in 2010, and people of different genders now receive different types of phishing and spam [86] **O9**.

Existing research primarily investigates binary (assumed cisgender) individuals, excluding non-binary and transgender people O1. Most papers mention only women and men, and few papers conduct statistical testing with non-binary individuals, often opting to filter them out during data processing. Non-binary people constitute a far smaller proportion of study participants, posing a challenge for parametric statistical testing that could be resolved with use of nonparametric tests or different study designs. Further, almost no papers discuss transgender individuals, while other work conflates gender and sex by referring to participants as female and male when discussing gender, against best practices [94]. Research should distinguish between cisgender and transgender people only when relevant, but given that transgender people experience significant harm [116] and erasure [108], omitting this aspect of gender may reflect cisnormativity.[6]

4.4 Age

Age granularity in the security literature varies from a single year to multiple decades and can be modeled as a numeric or categorical variable. Age is the second most studied sociodemographic factor (in 30 of 47 focus papers).

Prior work suggests that age may have been correlated with differences in password behaviors in the past, but is no longer T2. Two papers published after 2017 found no significant differences by age in switching password managers [66] or password reuse [77] (also found by a 2010 paper [99]). Supporting a theory of change in the past decade, a 2012 paper found that older users chose stronger passwords [3] but a study from the following year did not find such correlations [62]; similarly a 2011 paper found older users were more likely to share passwords [47], but evidence from a study seven years later did not support this finding [74],

Older users may behave more securely, while younger users focus on privacy T3. When studying a combined set of internet *security* behaviors, prior work found that older adults behaved more securely [118, 126], while younger users were more likely to adopt a combined set of *privacy* practices [126], e.g., use private browsing [29], use tracker blockers [60], and have Android lock screens [31] (though older users in Singapore may differ as they were more likely to adopt privacy practices [9]). The distinction between security and privacy behaviors may be partially explained by the finding that people 60+ were more likely to learn from automatic requirements or service providers than younger people [87]: formal sources may emphasize security as prevention of universal harm but privacy as a personal choice. Thus, older users were found to be more likely to enable 2FA in response to prompts [28] and deny Android permissions dialogs [2] as well as be more likely to be prompted by social triggers to behave securely [18]. However, differences by age were not found in responses to SSL warnings [106] or Android auto-updating [60].

With respect to online sharing, older users were more likely to post publicly than younger users [24] though less likely to specifically disclose distress during the COVID-19 pandemic [125] or share a security news event [19].

Similar to mixed results for phishing susceptibility by gender, prior work presents inconclusive findings about the relationship between age and phishing susceptibility O10. Three papers found that younger participants were more susceptible to phishing [36, 52, 100], while two found no correlations by age [21, 101].

4.5 Education

Formal education imparts knowledge and skills to students and increasingly includes information about computing. Educational systems and institutions vary greatly, including nationally and internationally, but can be broadly grouped into primary, lower and upper secondary, and tertiary (also called higher ed) [114].

Education does not seem to be correlated with secure behavior T4. Of the 14 papers that investigated relationships between education and security behaviors, four found significant correlations: more educated users were more likely to delete cookies and history [7] as well as adopt a composite of 30 security, privacy, and ID theft practices [126]. However,

[6] *Cisnormativity* is the assumption that everyone is or should be cisgender.

Table 3: Relationships between sociodemographic factors and security behaviors for papers in our focus dataset. For each sociodemographic factor (rows) and category of security behaviors (columns), we show X / Y, where X is the number of papers that found differences by factor for behavior, and Y is the total number of papers studying that factor and behavior. Summing counts do not sum to totals due to papers that study multiple factors or behaviors. Auth. = Authentication, Tech. Exp. = Technical Expertise, Composite = multiple behaviors studied together.

	Accounts & Auth.	**Device**	**Network & Web**	**Phishing & Spam**	**Social Media & Sharing**	**Composite**	**TOTAL**
Gender	6 / 9	4 / 6	3 / 4	3 / 6	10 / 10	3 / 4	28 / 38
Age	3 / 9	2 / 3	2 / 3	3 / 5	5 / 6	4 / 4	19 / 30
Education	- / 4	- / 2	1 / 2	- / 2	- / 1	3 / 3	4 / 14
Tech. Exp.	3 / 6	2 / 3	4 / 4	4 / 5	0 / 0	1 / 1	7 / 12
Geography	1 / 1	1 / 1	2 / 2	2 / 2	2 / 2	2 / 2	10 / 10
Internet Skill	2 / 2	- / -	1 / 1	2 / 4	1 / 1	1 / 1	7 / 9
Race	- / -	- / -	- / -	- / -	2 / 3	2 / 2	4 / 5
Income	- / 1	- / -	- / -	- / -	- / -	2 / 2	2 / 3
TOTAL	12	8	9	10	11	5	47

studying a composite of four behaviors to combat viruses and hackers, Wash et al. find that compared to those with a high school diploma, those who did not complete high school were more likely to adopt security behaviors [118]. Similarly, compared to those who held a BA, those who did not hold a BA were more likely to report learning security advice from automatic software updates [87].

On the other hand, 10 papers do not find significant correlations between education and account sharing [74], password strength [123], password reuse [77], switching of password managers [66], Android auto-updating [59], webcam cover use [56], public sharing behaviors on Snapchat [30], SSL warning behaviors [106], or phishing susceptibility [21, 52].

Differences in correlations between education and security behavior are not well understood. There may exist several reasons for these disparate results. First, while prior work notes that those with lower educations are more concerned about being the victim of a computer scam, losing financial information, and being the target of harassment [58], it is unclear how the varying computer knowledge held by those with different educational backgrounds affects the ability to employ secure behaviors. Education does not necessarily include computing or security education; indeed, prior work found that while people with less education rely on less authoritative sources of security advice, they report fewer negative incidents, perhaps suggesting that formal advice sources — including formal educational environments — fail to provide effective security education [88]. Further, a bachelor's degree education varies significantly by institution, such that high-level education categories reduce critical nuances. Education may not result in a linear increase in security behavior but may vary by context. Future work should investigate the relationships between education and security behaviors to better understand the underlying causal mechanisms at play.

There is a lack of research on students at levels besides secondary or post-secondary O3. Of 14 papers studying education and security behaviors, four conducted studies in U.S. and Canadian universities (e.g., university students, staff, faculty) and another seven conducted studies with U.S. recruitment/crowdworker populations, which are more likely to have attended or completed college than the average [38]. Only the remaining three papers were not conducted in the U.S. or Canada, revealing a striking over-representation of Western university-affiliated users in education-related results. Future work should consider a wider range of educational levels, in different or outside of educational systems.

4.6 Technical Expertise, Use, and Skill

Aside from general education, users have varying levels of experience with technology (i.e., technical expertise) or the internet specifically (i.e., internet skill).

Users with more technical expertise may use more technical security tools and take more protective actions T5. People with greater technical expertise were found to be more likely to use private browsing [29], identify security threats [71], and cite school (as opposed to required sources or device prompts) as a source of security advice [87]. Those with computer and mobile skills were more likely to take defensive security measures [7]. Greater technical expertise was also associated with higher adoption of multiple security practices [6, 42], although no correlation was found between technical expertise and webcam cover use [56].

Relatedly, internet use may suggest higher adoption of security practices, e.g., users who logged in from multiple locations chose stronger passwords [3], and users more active on Facebook were more likely to enable 2FA in response to prompts [28]. Prior work also demonstrates that people with more internet skill cite different sources of advice [87], which may contribute to these behavioral differences.

We observe an inconclusive relationship between technical expertise and password-related behaviors O12. Unlike other security behaviors, technical expertise did not have a clear relationship with password choices. Two papers studied

Table 4: A summary of trends and opportunities for future research from our literature review.

T#	Trends in Findings
T1	Women seem to focus more on information protection, while men seem to focus more on technical security.
T2	Older users may have had different password behaviors in the past, but no longer.
T3	Older users seem to exhibit more security-related behaviors while younger users focus more on privacy.
T4	Education does not seem to be correlated with secure behavior.
T5	Users with more tech expertise/use seem more likely to adopt technical security tools and take protective actions.
T6	Geography seems to be strongly correlated with differences in security behaviors.
O#	**Opportunities for Future Research**
Who is being studied: Lack of Focus around Specific Groups	
O1	Lack of research on non-binary and transgender people's security behaviors.
O2	Lack of research on gender differences in self-reported behaviors.
O3	Lack of research on education at levels besides (post-)secondary.
O4	Majority of papers conducted in U.S. and Western contexts; relative lack of research in other locations.
O5	Lack of research on geographical differences beyond granularity of countries.
O6	Lack of research on race and security behaviors.
O7	Lack of research on income and security behaviors.
What was found: Contradictory or Unclear Results	
O8	Mixed results on authentication behavior $\sim$ gender.
O9	Mixed results on phishing and spam susceptibility $\sim$ gender.
O10	Mixed results on phishing susceptibility $\sim$ age.
O11	Mixed results on phishing susceptibility $\sim$ internet skill.
O12	Mixed results on password behaviors $\sim$ technical expertise.
O13	Unclear patterns of geographical influence on security behaviors.
How: Methodological Issues	
O14	Significant interest in network/web behaviors and phishing/spam, but less on other behaviors.
O15	Security behaviors are primarily investigated through self-report methods.
O16	Many papers did not declare an interest in sociodemographic factors in the motivation of the work.
O17	Most papers had limited sample generalizability.

people affiliated with universities, one finding that participants in the computer science department chose stronger passwords than those in business [62], but the other found no conclusive evidence that technical expertise (including departmental affiliation) was correlated with stronger passwords [123]. Further, two papers found no correlation between technical expertise and password reuse [99] or password manager switching [66].

There is an inconclusive relationship between internet skill and phishing susceptibility O11. Two papers found that greater internet skill or knowledge about phishing correlated with less phishing or spam susceptibility [86, 100], while three others did not find correlations between internet skills or phishing susceptibility [21, 36, 101]. A potential explanation comes from outside the literature review: prior work suggests activity level on a platform (which is itself weakly correlated to internet skill) may have more explanatory power than the coarser measure of internet skill [86].

4.7 Geography and Race

Geography is a proxy and umbrella term for a range of sociodemographic factors, including nationality, language, population density, political history, culture, internet penetration, freedom of speech, and more. Geography also shifts over time since politics and culture reshape the societies living between socially constructed boundaries.

Race refers to groups of people who share cultural, social, and physical similarities. It has been shaped through historical narratives of identity to be a tool of power, particularly for discrimination and the justification of colonialism [68, 90, 105]. Though racialized science continues to advance myths of biological differences between races, race is a powerful determinant of the privileges that an individual has access to, e.g., education, wealth, health.

All papers in our focus dataset studying geographic factors with respect to security behaviors were significantly correlated with behaviors T6, but effects lacked clear cross-cultural patterns O13. While the ten papers investigating correlations between geography and security behaviors find differences in many types of behaviors, these results are often sparsely populated, and it is not clear why these patterns appear or how they do, or do not, generalize to other geographical regions. German and French participants were found to be twice as likely to take protective actions against tracking than those in the UK [13]. Compared to U.S. and U.K. users, German internet users tended to adopt more advanced, active privacy methods, such as proxies, Tor, and providing false information [12]. U.S. users were more likely to take security-protective actions because of proactive triggers, whereas people in India were more likely to act in response to social triggers [18]. Password strength varied by primary language spoken: passwords chosen by Indonesian-speaking users were found to be the weakest; German- and Korean-speaking users tended to choose relatively strong passwords [3]. Android lock screen usage also varied by country, e.g., 76.4% in the U.K. compared to 50.4% in Italy [31].

Phishing and spam susceptibility also differed by geographic location. Users who live in countries that have more spam are less likely to click it [86]. South Koreans were more likely to fall for phishing attacks in Korean than English, while Japanese participants were more likely to fall for phishing in English than Japanese [36]. On social media, rural U.S. users were more likely to set profiles to private than urban U.S. users [27], and Saudi women were more likely to block people on WhatsApp than Indian women [20]. Compared to U.S. users, U.K. users were less likely to dismiss cookie banners but more likely to not read consent text [4].

Few papers discuss geographical factors beyond the granularity of a country O5. Geographical factors describe a wide range of sociodemographic variance beyond national identity; however, the majority of papers focus only on these differences. Of ten papers, eight segregate geographical differences by nationalities [4, 13, 18, 20, 31, 36, 86], while only two discuss variations by language spoken [3, 36], and only one considers urbanization differences within the same country [27]. Future work can continue to illuminate how security behavior changes based on sociodemographics other than national identity, such as within a country, in cultures that extend beyond nations, or WEIRD vs. non-WEIRD societies [55].

Race is an infrequently studied sociodemographic factor in research on security behaviors O6. Race is a function of culture and was only studied in five papers. Trends are difficult to ascertain because these papers investigated distinct behaviors and used different racial categorizations (we report using those papers' terminology). With respect to security, prior work found that white people were more likely to take certain protective security actions than Asian Americans and Pacific Islanders as well as Black or African Americans, though American Indians and Alaska Natives were more likely than white people to use security settings [118]. White people were more likely to solicit security advice from family and friends than Hispanic people [87]. With respect to privacy, while one paper found that racial minorities were more likely to publicly post on Snapchat [30], another found that compared to African Americans, white people were more likely to disclose distress on social media [125]. One paper did not find racial differences in Facebook profile privacy settings [74].

4.8 Income

Income determines not only the financial resources that one has to spend, but it may also indirectly influence the time or energy that one can put towards security behaviors.

More research is needed on relationships between income and security behaviors O7. Only three papers studied relationships between income and security behaviors: one found no differences in account sharing [74], while another found that people with lower incomes were more likely to adopt a combined set of security and privacy behaviors [126]. People at different income levels learn from different sources; those with higher incomes were more likely to learn from school, work, or device prompts [87].

5 Guidelines for Future Sociodemographic Research on Security Behaviors

Our literature review documents a significant and growing interest in studying how sociodemographic factors relate to security behavior. Based on our review, our own domain expertise, and sustained discussions amongst the research team, we developed guidelines to support strong and valuable research contributions. We iteratively refined these guidelines throughout our research process, including during our measurement study (see Section 6). We offer these guidelines to assist researchers in both their research and reviewing process. However, we caution: the guidelines are not a checklist to guarantee quality work, there may be cases when they do not apply, and norms and best practices continually evolve.

Factor Selection. The selection of which sociodemographic factors to analyze should be done deliberately and stated as a research interest in the motivation (e.g., in the introductory section) for the work. Many papers in our literature review did not explicitly declare studying sociodemographic differences but presented correlations with sociodemographic factors in the results (see Section 4.2), which may indicate spurious correlations **O16**. Additionally, multiple studies are necessary to establish robust evidence of factor correlations, as demonstrated by the replication crisis in psychology research [61, 102].

G1: Identify at the beginning of the study the specific sociodemographic factors, if any, you intend to study. If you investigate sociodemographic differences, commit to reporting the results even if they do not show differences, i.e., null results. Consider study pre-registration [10].

Group Selection. Within all sociodemographic factors, there are groups that are privileged or marginalized. We found many opportunities for research about different groups, e.g., groups marginalized by gender (see Section 4.3) **O1** or race (see Section 4.7) **O6**. Researchers choose to study a subset of groups for practical or other reasons. If so, describe how the scope was chosen and how the sample studied relates to the broader population.

G2: Consider and justify which groups are included in or excluded from your study.

Method Selection. Epistemic diversity allows researchers to explore a wider range of research questions. Consider research methods that make different types of contributions [124], including but not limited to: quantitative, qualitative, or mixed

methods [53]; descriptive, experimental, or speculative; cross-sectional or longitudinal [15, 26]. If relevant, consider causal inference methods [17, 76].

Most papers in our literature review used statistical hypothesis testing, which is primarily valuable to identify factors for correlations but not causation. Few papers in our literature review modeled sociodemographic factors as control factors (see Cho et al. as an exception [9]). Further, many papers we reviewed used self-report methods **O15**, which are convenient for formative work but not suitable for establishing robust results.

G3: Consider using diverse research methods, acknowledging the benefits and limitations of each.

Result Interpretation. When interpreting results, remember that complex factors could lead to any observed differences. Avoid "essentializing" (reducing individuals to assumed group characteristics) and over-generalizing findings. In interpreting results, state not only what can be implied from the results, but also what cannot: for example, "We found a significant correlation between this factor and this behavior, which might be due to methodological choices or factors outside the scope of this study." This is particularly important for studies conducted on limited samples **O17**.

G4: When sociodemographic differences are observed, exercise caution in describing the results. Consider posing several causal interpretations for observed differences.

Author Positionality. Weighing the advantages and disadvantages of disclosure [54], if appropriate and safe to do so, include positionality statements in your work. In some cases, the risks to researchers may not merit disclosure. Further, we caution against positionality statements that merely list identities without reflexivity as to how these identities influenced the research process. When included thoughtfully, such statements provide context for readers about researcher motivations and the potential influence of researcher backgrounds. For example, a majority of existing research in our literature review is U.S.-centric and studies people affiliated with universities **O3** and **O4**, which is likely the result of the (undiscussed) positionality of researchers as primarily professors and graduate students at Western universities.

G5: Be aware of your own positionality and identity as a researcher and critically reflect on how it might affect your research questions, hypotheses, and interpretation of your findings [40].

6 Case Study: Measuring Sociodemographics and Security Behaviors on Facebook

We now instantiate our guidelines in our own case study to concretely demonstrate their application for future researchers. We iteratively refined the guidelines in the process, resulting in the version in Section 5.

Unlike most prior work that uses self-reports, we leverage de-identified, aggregated log data to shed light on how users' real security behavior correlates with sociodemographic factors. Security is often a secondary goal, so users may incorrectly recall actions and self-report based on social desirability [50, 67] or researcher demand [72]. Thus, real-world security behavior offers high ecological validity and an important complement to self-report studies.

6.1 Measurement Methods

This study was conducted by combining de-identified, aggregated log data about security behavior with the results of a 16,829 respondent survey run on Facebook in 16 countries during December 2019. Respondents were recruited through both web and mobile interfaces via a message at the top of their social media feeds. The survey was translated into the respondent's local language by professional translators with native language proficiency.

Our *dependent variables (DVs)* were four security behaviors: **Security settings visited** ($\pm$ 45 days of survey date), **Security settings acted on** ($\pm$ 45 days of survey date, only among respondents who visited), **2FA enabled** (ever), and **Stronger password** (i.e., those not yet identified as potentially more vulnerable to attack[7]).

Based on the available log data about Facebook users, we chose six sociodemographic factors to study **G1**. These factors were: **Age**, **Gender** (binary[8]), **Educational attainment**, **Geographic location** (16 countries in four regions), **Internet skill**, and **Technical knowledge**. Appendix B.1 details these factors and how they were determined. We also included four available *independent variables (IVs)* regarding Facebook use based on the de-identified platform data: **Tenure** (how long the respondent had an account), **L30** (how many of the last 30 days the respondent had logged in to their account), **Time spent** (how much time the respondent spent on the platform over the last 30 days), and **Friend count** (number of social connections on the platform).

Analysis. We analyzed our data with logistic regression models because of the scale of our data **G3**. We weighted our

[7] See https://www.facebook.com/help/124904560921566 for details on Facebook's password guidelines and https://www.facebook.com/notes/760840091433907/ on identifying potentially vulnerable passwords.

[8] Due to cross-cultural differences in prevalence of non-binary gender reporting, we study only those who reported a binary gender to allow for interpretable comparisons across countries. As underscored in **O1**, we encourage future work on those of non-binary genders.

sample to represent the population of the broader social media platform on age, gender, tenure, and L30 in order to maximize the generalizability of our results. To examine the relationship between security behavior and our independent variables, we constructed weighted logistic regression models, with security behavior as the boolean DV and the other variables listed above as the IVs (see Appendix B.2). We also controlled for two interactions that had correlations with $\rho > 0.3$: *l30∗time spent* — there is a correlation between the number of days and amount of time spent on the platform — and *location∗tenure* — there is a correlation between geographic location and platform tenure since the platform was introduced to different markets at different times. Regression models were fit using 5-fold cross validation. The variance in AIC between the five folds was always less than 3%.

Limitations. Our measurement study considers users of only one social media platform, although this platform is one of the largest and most diverse online platforms. Though we studied users in 16 countries, this represents a minority of countries globally **G2**. Further, racial categories differ greatly by sociocultural context, which is why our measurement study across 16 countries did not study race **G2**.

Ethics. We analyze de-identified, aggregated log data of users on Facebook who voluntarily completed survey data. There was no manipulation of any user's experience, and no personal identifying information was used. Our research procedures were vetted and approved through an internal review process.

Positionality. We echo our positionality statement from Section 3.4 in conducting this measurement work **G5**. Additionally, we note that one author engaged in a paid collaboration with Meta, which allowed them to access and analyze the de-identified, aggregated log data.

6.2 Measurement Results

In interpreting our results, we emphasize that all findings describe only associations between sociodemographics and behaviors, and we do not make causal claims **G4**.

Gender: On Facebook, women were more likely than men to take action regarding security settings, but no gender differences were found with respect to password strength or use of 2FA. We do not find significant differences in likelihood to *visit* security settings, but women were more than 1.4 times as likely to *action* security settings than men ($OR = 1.44, p < .01$). These results may support **T1** if actioning security settings is interpreted as an information protection behavior. Given that other work on the same platform we study finds that people tend not to make a clear distinction between security and privacy [85], women actioning security settings would align with other information protection behaviors. We found no significant differences in likelihood to have a stronger password or use 2FA by gender. While this null result could mean there is no relationship between gender and these behaviors, it could also mean that Facebook users are unique in not having gender differences, but differences could be found in studies of users of other services.

Age: While older Facebook users were less likely to visit their security settings, action their security settings, and use 2FA, those age 50+ were more likely to use stronger passwords. Compared to those aged 25-34, older adults were significantly less likely to *view* their security settings, with the odds of those between 35-49 being 0.74 times as likely to visit their security settings ($OR_{35-49} = 0.74, p_{35-49} < .05$) and those 50+ being 0.63 times as likely ($OR_{50+} = 0.63, p_{50+} < .05$). We also found significant differences in their use security settings, with the odds of older adults *actioning* their security settings being lower ($OR_{35-49} = 0.55, p_{35-49} < .001$; $OR_{50+} = 0.38, p_{50+} < .001$) and the odds of them using 2FA being lower, as well ($OR_{35-49} = 0.79, p_{35-49} < .05$; $OR_{50+} = 0.63, p_{50+} < .05$). However, the odds of adults 50+ having a stronger password was higher ($OR_{50+} = 2.08, p_{50+} < .05$). These findings appear to support **T2**, i.e., that older adults are more likely than younger to adopt security behaviors like passwords.

Education: On Facebook, education levels were correlated with the likelihood of using 2FA. Compared to users with no post-secondary education, users with some college ($OR = 7.14, p < .01$) or a bachelor's degree or more ($OR = 5.40, p < .01$) were more likely to use 2FA. However, education *was not* correlated with visiting or actioning security settings or having a stronger password, in alignment with **T4**.

It is possible that users with higher educational levels had to previously comply with their institution's 2FA IT policy and thus were more likely to reengage with 2FA on Facebook. Those with higher educations may also be more comfortable with computer systems and security tools like 2FA. Future work can continue to investigate post-secondary institution's influence on 2FA adoption by comparing with users not affiliated with post-secondary institutions, towards **O3**.

Technical expertise: On Facebook, technical expertise was correlated with stronger passwords and 2FA use. Technical knowledge of passwords was correlated with having a stronger password ($OR = 1.88, p < .05$) and using 2FA ($OR = 1.33, p < .05$), as was knowledge of the reaction feature on Facebook ($OR = 1.75, p < .05$; $OR = 1.37, p < .01$for stronger password and 2FA, respectively). Knowledge of QR codes was also correlated with greater use of 2FA ($OR = 1.49, p < .001$), while knowledge of downloads was not correlated with any security behavior. Since downloads are the oldest technology feature we asked about, the trends we find in our measurement study seem in alignment with our literature review, i.e., that technical expertise correlates with increased likelihood to take secure actions **T5**.

Internet skill: On Facebook, internet skill was correlated

with all behaviors except having a stronger password. Internet skill was correlated with visiting ($OR = 1.41, p < .01$) and actioning ($OR = 1.44, p < .05$) security settings as well as using 2FA ($OR = 1.84, p < .001$).

Platform-specific use: Tenure on a platform was correlated with all security behaviors, while use in the past 30 days was not correlated with any. Platform tenure in years was correlated with all four security behaviors, specifically to be less likely to visit ($OR = 0.95, p < .01$) or action ($OR = 0.95, p < .05$) security settings, less likely to have a stronger password ($OR = 0.91, p < .05$), but more likely to use 2FA ($OR = 1.84, p < .001$). This may be due to those with longer standing accounts having already adjusted their settings and due to changes over time in password advice (those creating accounts earlier may have received less password education at the time of account creation). Friends and time spent were also positively correlated with use of 2FA ($OR = 1.02, p < .01$; $OR = 1.13, p < .05$), though use in the last 30 days was not correlated with any security behaviors.

Geography: On Facebook, users in Africa, the Middle East, and Asian geographic markets differed significantly from the Western market in terms of security behavior. The odds of users in Asia visiting security settings were higher than users in the West ($OR = 1.94, p < .05$), lower compared to the same group to have a stronger password ($OR = 0.16, p < .001$), and no different for actioning security settings and using 2FA. Users in Africa and the Middle East were less likely to have a stronger password ($OR = 0.24, p < .05$), but other behaviors were not significantly different. Users in Latin America were not significantly different from Western users on any of the four security behaviors we studied. Geographic differences in our case study broadly align with **T6**, i.e., that geographic differences are significant but with unclear patterns **O13**.

7 Discussion

Having presented a systematization of knowledge of sociodemographics and security behaviors (Section 4) and guidelines for researchers (Section 5) and applied them in our own measurement study (Section 6), we now critically consider our *lack* of knowledge in this space.

7.1 The Missing "Why?"

This work reveals many correlations between sociodemographic factors and security behaviors, but little insight into *why* these correlations exist. The trends we synthesize and the opportunities we highlight begin to pose hypotheses for underlying causal relationships, but much work remains. Without understanding why, interpreting results becomes arduous and different studies can yield seemingly contradictory results. For example, when correlational studies find that one sociodemographic group adopts a security behavior less than another, is this the result of sample differences, different threat models, user interface designs that assumed one group as "default" users [14], or some other reason? Sociodemographic factors also do not exist in isolation but are correlated and influence each other; though this work did not investigate (reflecting papers in our literature review) intersectionality [16], only through understanding *why* each identity influences behavior can intersectional analyses be conducted.

Drawing implications for interventions to change behavior when the *why* is still missing is a tenuous proposition. We can neither know what interventions might encourage adoption of security behaviors nor whether such interventions are necessary, desired, or even helpful. Worse, if we assume incorrectly, subsequent actions or discussions may have a negative impact, e.g., perpetuating gendered stereotypes about computer security and privacy behaviors [119]. Recent related work on underlying causes of differences in security threats, rather than on behaviors, takes initial steps toward a causality-focused framework, e.g., identifying higher-order factors like prominence and marginalization that put particular groups at higher risk of security threats [93, 117].

7.2 Towards Answering "Why?"

What should be next for this field of research on sociodemographics and computer security and privacy? To close the knowledge gap, future work should explore not only *what* differences exist among sociodemographic groups in security and privacy, but *why* these differences exist.

Epistemic Diversity of Methods. Seeking to understand the causal relationships underlying sociodemographics and security behaviors cannot be achieved solely through quantitative methods. That does not mean establishing correlations has no value; the field as a whole must grapple with *why*, and individual papers provide incremental steps towards an answer.

In addition to the inferential methods used in the quantitative papers we analyzed, qualitative methods, e.g., in-depth interviews, observational studies, and ethnographies, can be used to explore the missing *why*. Such methods are increasingly used in security and privacy research to study the needs and practices of specific marginalized and vulnerable user groups but should also be used to draw out the underlying sociodemographic factors and their relationships to behavior. Especially by critically comparing privileged and marginalized groups, qualitative methods can assess existing hypotheses about causal relationships or pose new relationships and mechanisms of effect.

There are also other quantitative methods to consider beyond correlation and regression analyses. For example, structured equation modeling (SEM) involves constructing a model with causal relationships and statistically evaluating relationships as well as effect magnitudes [113]. Other analyses in-

clude causal inference methods [75], Bayesian methods [51], or quantitative meta-analyses. Each method has strengths and limitations that future work can explore.

Towards Social Theories. Overall, we recommend that security and privacy researchers learn from other fields that rely on social theories. Social theories, i.e., scientifically plausible principles that seek to explain certain phenomena by posing causal hypotheticals, pose richer explanations for how people behave, which avoids essentializing a group of people. For example, when women take fewer security measures than men, some might interpret this to mean that men are fundamentally better suited to security tasks. Instead, women's choices may reflect systemic educational inequities, where women were discouraged from learning about technical topics, or other reasons. Research must be careful to avoid attributing differences to innate group characteristics, e.g., racial essentializing [90]. Relevant social theories support robust interpretation when differences are found and can also indicate how a lack of difference can be meaningful.

Social theories from other fields can also help illuminate gaps in security behavior research, i.e., understudied factors that also merit study. Papers we analyzed focused most often on factors such as gender and age, but factors that have been more deeply studied in other fields and could inform security research include (dis)ability, marital status, religion, migration status, socioeconomic status, and race.

Finally, social theories facilitate critically challenging assumptions inherent in some perspectives on sociodemographics and security. This includes (1) questioning whether certain security behaviors are desirable for certain groups and in certain contexts since "spending more time on security is not an inherent good" [37]. Further, (2) the security behaviors studied may not address (or be trusted to address) the needs of all communities, especially those most marginalized [64, 121], and (3) sociodemographic categorizations themselves, and the types of security behaviors studied, are not the only ways to organize the space and may not be the most salient to users. As research continues to explore sociodemographic differences in security, incorporating theoretically informed inquiries presents the greatest opportunity to build on current methods and knowledge.

8 Related Work

Qualitative Studies of Marginalized Populations in Security and Privacy. A sizeable and growing body of literature investigates the experiences, behaviors, and needs of populations underrepresented in security and privacy research. These works often overlap with sociodemographic factors, e.g., targets of intimate partner violence [112] who are disproportionately women, refugees [104], LGBTQ+ individuals [25], and Muslim-American women [92]. Other studies investigate vulnerable populations due to their work, e.g., journalists [65], content creators [110], and sex workers [64]. These studies have been overwhelmingly qualitative, i.e., providing rich insights rather than quantitatively generalizable results.

Meta-Analyses of User Studies. The need for cross-study synthesis grows as the number of user studies of security behavior increases, e.g., about which methods are common [22], or expert vs. non-expert users [46]. Prior meta-analyses also investigated marginalized [93] and at-risk users [117], specifically developing unifying frameworks. We focus on sociodemographics as the unifying frame because they are a powerful latent cause of differences; ultimately, marginalization relies on our contemporary, socially constructed sociodemographic categories. Aside from a recent preprint investigating geographic diversity in security and privacy research [35], we are unaware of other meta-reviews taking a sociodemographic lens, though sociodemographic meta-reviews in HCI are more common, e.g., culture [44] as well as gender, race, and class [96].

9 Conclusion

We broadly survey scholarship (151 papers) that quantitatively studies sociodemographic factors and computer security behaviors, and we synthesize methods and results in a focused review of 47 papers. Taking a critical demography approach, we enumerate five trends in existing research and fifteen opportunities for future research (Table 4). We establish five guidelines for conducting quality sociodemographic research investigating security behaviors (Section 5) and apply those guidelines in a case study of the real security behaviors of 16,829 Facebook users. Taken together, this work documents the current state of knowledge on how people's identities relate to the security and privacy actions they take and charts new directions towards greater security, privacy, and equity.

10 Acknowledgements

We thank our reviewers and especially our shepherd for their helpful feedback. We are also grateful to Alannah Oleson, Matthias Fassl, and the UW Security and Privacy Research Lab (including Rachel Hong, Alexandra E. Michael, Christina Yeung) for insightful conversations on framing, methods, and impact. We thank Maximilian Golla and Aleksei Stafeev for sharing an NDSS paper archive. This work was supported in part by the U.S. National Science Foundation under Awards 2205171 and 2206950 and the Graduate Research Fellowship Program (DGE-1746047). The fifth author did a portion of this work while working as a contractor for Meta.

References

[1] R. Bivens. The gender binary will not be deprogrammed: Ten years of coding gender on Facebook. *New Media & Society*, 2017.

[2] B. Bonné, S. T. Peddinti, I. Bilogrevic, and N. Taft. Exploring decision making with Android's runtime permission dialogs using in-context surveys. In *Proc. SOUPS*, 2017.

[3] J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Proc. IEEE S&P*, 2012.

[4] E. R. Bouma-Sims, M. Li, Y. Lin, A. Sakura-Lemessy, A. Nisenoff, E. Young, E. Birrell, L. F. Cranor, and H. Habib. A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile. In *Proc. CHI*, 2023.

[5] G. C. Bowker and S. L. Star. *Sorting Things Out: Classification and its Consequences*. MIT Press, 2000.

[6] K. Busse, J. Schäfer, and M. Smith. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Proc. SOUPS*.

[7] J. Chen, M. Paik, and K. McCabe. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *SOUPS*, 2014.

[8] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle. Multiple password interference in text passwords and click-based graphical passwords. In *Proc. CCS*, 2009.

[9] H. Cho and A. Filippova. Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study. In *Proc. CSCW*, 2016.

[10] A. Cockburn, C. Gutwin, and A. Dix. HARK No More: On the Preregistration of CHI Experiments. In *Proc. CHI*, 2018.

[11] P. H. Collins. *Fighting Words: Black Women & The Search for Justice*. Uniersity of Minnesota Press, 1998.

[12] K. P. Coopamootoo. Usage patterns of privacy-enhancing technologies. In *Proc. CCS*, 2020.

[13] K. P. Coopamootoo, M. Mehrnezhad, and E. Toreini. "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. In *Proc. USENIX Security*, 2022.

[14] S. Costanza-Chock. *Design Justice: Community-Led Practices to Build the Worlds We Need*. MIT Press, 2020.

[15] C. Courage, J. Jain, and S. Rosenbaum. Best Practices in Longitudinal Research. In *CHI Extended Abstracts*, 2009.

[16] K. W. Crenshaw. *On intersectionality: Essential writings*. The New Press, 2017.

[17] S. Cunningham. *Causal inference: The mixtape*. Yale University Press, 2021.

[18] S. Das, L. A. Dabbish, and J. I. Hong. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proc. SOUPS*, 2019.

[19] S. Das, J. Lo, L. Dabbish, and J. I. Hong. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proc. CHI*, 2018.

[20] J. Dev, P. Moriano, and J. L. Camp. Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations. In *Proc. SOUPS*, 2020.

[21] R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing Works. In *Proc. CHI*, 2006.

[22] V. Distler, M. Fassl, H. Habib, K. Krombholz, G. Lenzini, C. Lallemand, L. F. Cranor, and V. Koenig. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 2021.

[23] M. Fenniak, M. Stamy, pubpub zz, M. Thoma, M. Peveler, exiledkingcc, and pypdf Contributors. The pypdf library.

[24] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert. What (or Who) Is Public? Privacy Settings and Social Media Content Sharing. In *Proc. CSCW*, 2017.

[25] C. Geeng, M. Harris, E. Redmiles, and F. Roesner. "Like Lesbians Walking the Perimeter": Experiences of US LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *Proc. USENIX Security*, 2022.

[26] J. Gerken. *Longitudinal Research in Human-Computer Interaction*. PhD thesis, Universität Konstanz, 2011.

[27] E. Gilbert, K. Karahalios, and C. Sandvig. The network in the garden: an empirical analysis of social media in rural life. In *Proc. CHI*, 2008.

[28] M. Golla, G. Ho, M. Lohmus, M. Pulluri, and E. M. Redmiles. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *Proc. USENIX Security*, 2021.

[29] H. Habib, J. Colnago, V. Gopalakrishnan, S. Pearman, J. Thomas, A. Acquisti, N. Christin, and L. F. Cranor. Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing. In *Proc. SOUPS*, 2018.

[30] H. Habib, N. Shah, and R. Vaish. Impact of Contextual Factors on Snapchat Public Sharing. In *Proc. CHI*, 2019.

[31] M. Harbach, A. De Luca, N. Malkin, and S. Egelman. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proc. CHI*, 2016.

[32] E. Hargittai and Y. P. Hsieh. Succinct survey measures of web-use skills. *Social Science Computer Review*, 30(1):95–107, 2012.

[33] E. Hargittai and E. Litt. New Strategies for Employment? Internet Skills and Online Privacy Practices during People's Job Search. *IEEE Security & Privacy*, 11(3):38–45, 2013.

[34] R. Hasan, B. I. Bertenthal, K. Hugenberg, and A. Kapadia. Your Photo is so Funny that I don't Mind Violating Your Privacy by Sharing it: Effects of Individual Humor Styles on Online Photo-sharing Behaviors. In *Proc. CHI*, 2021.

[35] A. A. Hasegawa, D. Inoue, and M. Akiyama. A Survey on the Geographic Diversity of Usable Privacy and Security Research. *arXiv*, 2023.

[36] A. A. Hasegawa, N. Yamashita, and N. Akiyama. Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails. In *Proc. SOUPS*, 2021.

[37] C. Herley. More is not the answer. *IEEE Security and Privacy*, January 2014.

[38] P. Hitlin. Research in the Crowdsourcing Age, a Case Study. Technical report, Pew Research Center, July 2016.

[39] A. L. Hoffmann. Terms of inclusion: Data, discourse, violence. *New Media & Society*, 2021.

[40] H. D. Horton. Critical demography: The paradigm of the future? In *Sociological Forum*, 1999.

[41] R. Hoyle, S. Das, A. Kapadia, A. J. Lee, and K. Vaniea. Viewing the Viewers: Publishers' Desires and Viewers' Privacy Concerns in Social Networks. In *Proc. CSCW*, 2017.

[42] I. Ion, R. Reeder, and S. Consolvo. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *SOUPS*. USENIX Association, 2015.

[43] H. Jia, P. J. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll. Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In *Proc. CSCW*, 2015.

[44] M. Kamppuri, R. Bednarik, and M. Tukiainen. The Expanding Focus of HCI: Case Culture. In *Proc. NordiCHI*, 2006.

[45] N. Karusala, A. Bhalla, and N. Kumar. Privacy, Patriarchy, and Participation on Social Media. In *Proc. DIS*, 2019.

[46] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig. Human factors in security research: Lessons learned from 2008-2018.

[47] J. J. Kaye. Self-reported password sharing strategies. In *Proc. CHI*, 2011.

[48] O. Keyes. The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. *CSCW*, 2018.

[49] O. Keyes, C. May, and A. Carrell. You Keep Using That Word: Ways of Thinking about Gender in Computing Research. *CSCW*, 2021.

[50] I. Krumpal. Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & quantity*, 47(4):2025–2047, 2013.

[51] J. Kruschke. *Doing Bayesian data analysis: A tutorial with R, JAGS, and Stan*. Academic Press, 2014.

[52] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of Phish: A Real-World Evaluation of Anti-Phishing Training. In *Proc. SOUPS*, 2009.

[53] J. Lazar, J. H. Feng, and H. Hochheiser. *Research Methods in Human-Computer Interaction*. Morgan Kaufmann, 2017.

[54] C. Liang, S. A. Munson, and J. A. Kientz. Embracing Four Tensions in Human-Computer Interaction Research with Marginalized People. *TOCHI*, 28(2), 2021.

[55] S. Linxen, C. Sturm, F. Brühlmann, V. Cassau, K. Opwis, and K. Reinecke. How WEIRD is CHI? In *Proc. CHI*, 2021.

[56] D. Machuletz, S. Laube, and R. Böhme. Webcam Covering as Planned Behavior. In *Proc. CHI*, 2018.

[57] M. Madden. Privacy management on social media sites. *Pew Internet Report*, 24:1–20, 2012.

[58] M. Madden. Privacy, security, and digital inequality, 2017.

[59] A. Mathur and M. Chetty. Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates. In *Proc. SOUPS*, 2017.

[60] A. Mathur, J. Vitak, A. Narayanan, and M. Chetty. Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking. In *Proc. SOUPS*, 2018.

[61] S. E. Maxwell, M. Y. Lau, and G. S. Howard. Is psychology suffering from a replication crisis? what does "failure to replicate" really mean? *American Psychologist*, 70(6):487, 2015.

[62] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. Measuring Password Guessability for an Entire University. In *Proc. CCS*, 2013.

[63] K. S. McClure. *Selecting and Describing Your Research Instruments*, chapter Identifying and defining the constructs and variables to measure. American Psychological Association, 2020.

[64] A. McDonald, C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles. "It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online. In *Proc. USENIX Security*, 2021.

[65] S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *Proc. USENIX Security*, 2015.

[66] C. W. Munyendo, P. Mayer, and A. J. Aviv. "I just stopped using one and started using the other": Motivations, Techniques, and Challenges When Switching Password Managers. In *Proc. CCS*, 2023.

[67] A. J. Nederhof. Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, 15(3):263–280, 1985.

[68] E. B. of the American Anthropological Association. AAA Statement on Race.

[69] A. Oleson, B. Xie, J. Salac, J. Everson, F. M. Kivuva, and A. J. Ko. A Decade of Demographics in Computing Education Research: A Critical Review of Trends in Collection, Reporting, and Use. In *Proc. ICER*, 2022.

[70] K. Olmstead and A. Smith. What the public knows about cybersecurity. *Pew Research Center*, 22, 2017.

[71] K. Onarlioglu, U. O. Yilmaz, E. Kirda, and D. Balzarotti. Insights into User Behavior in Dealing with Internet Attacks. In *NDSS*, 2012.

[72] M. T. Orne. On the social psychology of the psychological experiment: With particular reference to demand characteristics and their implications. *American psychologist*, 17(11):776, 1962.

[73] A. A. C. Ortega. Toward critical demography 2.0. *Human Geography*, 2023.

[74] C. Y. Park, C. Faklaris, S. Zhao, A. Sciuto, L. Dabbish, and J. Hong. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proc. SOUPS*, 2018.

[75] J. Pearl. Causal inference in statistics: An overview. *Statistics Surveys*, 2009.

[76] J. Pearl, M. Glymour, and N. P. Jewell. *Causal inference in statistics: A primer*. John Wiley & Sons, 2016.

[77] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *CCS*, CCS, pages 295–310, New York, NY, USA, 2017. Association for Computing Machinery. event-place: Dallas, Texas, USA.

[78] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor. Why people (don't) use password managers effectively. In *SOUPS*, 2019.

[79] D. L. Poston, editor. *Handbook of population*. Springer, 2nd edition, 2019.

[80] S. H. Preston, P. Heuveline, and M. Guillot. *Demography: measuring and modeling population processes*. Blackwell, 2001.

[81] H. C. Purchase. *Experimental human-computer interaction: a practical guide with visual examples*. Cambridge University Press, 2012.

[82] E. M. Redmiles. Net Benefits: Digital Inequities in Social Capital, Privacy Preservation, and Digital Parenting Practices of US Social Media Users. In *AAAI*, 2018.

[83] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek. A summary of survey methodology best practices for security and privacy researchers. 2017.

[84] E. M. Redmiles, M. M. Bennett, and T. Kohno. Power in Computer Security and Privacy: A Critical Lens. *IEEE Security & Privacy*, March/April 2023.

[85] E. M. Redmiles, J. Bodford, and L. Blackwell. "I just want to feel safe": A Diary Study of Safety Perceptions on Social Media. In *Proc. ICWSM*, 2019.

[86] E. M. Redmiles, N. Chachra, and B. Waismeyer. Examining the Demand for Spam: Who Clicks? In *Proc. CHI*, 2018.

[87] E. M. Redmiles, S. Kross, and M. L. Mazurek. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *Proc. CCS*, 2016.

[88] E. M. Redmiles, S. Kross, and M. L. Mazurek. Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proc. CHI*, 2017.

[89] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *Proc. USENIX Security*, 2020.

[90] A. Saini. *Superior: The Return of Race Science*. Penguin Random House, 2019.

[91] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[92] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. S. Gaytán-Lugo, T. Matthews, S. Consolvo, and E. Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proc. SOUPS*, 2018.

[93] S. Sannon and A. Forte. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. *CSCW*, 2022.

[94] M. K. Scheuerman, K. Spiel, O. L. Haimson, F. Hamidi, and S. M. Branham. HCI Gender Guidelines, 2020.

[95] M. K. Scheuerman, K. Wade, C. Lustig, and J. R. Brubaker. How We've Taught Algorithms to See Identity: Constructing Race and Gender in Image Databases for Facial Analysis. *CSCW*, 2020.

[96] A. Schlesinger, W. K. Edwards, and R. E. Grinter. Intersectional HCI: Engaging identity through gender, race, and class. In *Proc. CHI*, 2017.

[97] J. C. Scott. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press, 2020.

[98] M. Sharif, J. Urakawa, N. Christin, A. Kubota, and A. Yamada. Predicting Impending Exposure to Malicious Content from User Behavior. In *Proc. CCS*, 2018.

[99] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proc. SOUPS*, 2010.

[100] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proc. CHI*, 2010.

[101] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *ACM International Conference Proceeding Series*, volume 229, pages 88–99, 2007.

[102] P. E. Shrout and J. L. Rodgers. Psychology, Science, and Knowledge Construction: Broadening Perspectives from the Replication Crisis. *Annual Review of Psychology*, 69:487–510, 2018.

[103] W. Sigle. Demography's theory and approach: (How) has the view from the margins changed? *Population Studies*, 75(sup1):235–251, 2021.

[104] L. Simko, A. Lerner, S. Ibtasam, F. Roesner, and T. Kohno. Computer Security and Privacy for Refugees in the United States. In *Proc. IEEE S&P*, 2018.

[105] A. Smedley and B. D. Smedley. Race as biology is fiction, racism as a social problem is real: Anthropological and historical perspectives on the social construction of race. *American Psychologist*, 60(1):16, 2005.

[106] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings. In *Proc. SOUPS*, 2011.

[107] F. Stutzman and J. Kramer-Duffield. Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. In *Proc. CHI*, 2010.

[108] M. I. Suárez and P. Slattery. Resisting erasure: Transgender, gender nonconforming, and nonbinary issues in curriculum studies. *Journal of Curriculum and Pedagogy*, 15(3):259–262, 2018.

[109] R. Sáenz and M. C. Morales. *Handbook of Population*, chapter Demography of Race and Ethnicity. Springer, 2nd edition, 2019.

[110] K. Thomas, P. G. Kelley, S. Consolvo, P. Samermit, and E. Bursztein. "It's common and a part of being a content creator": Understanding How Creators Experience and Cope with Hate and Harassment Online. In *Proc. CHI*, 2022.

[111] S. Tifferet. Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93:1–12, 2019.

[112] E. Tseng, M. Sabet, R. Bellini, H. K. Sodhi, T. Ristenpart, and N. Dell. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proc. CHI*, 2022.

[113] J. B. Ullman and P. M. Bentler. Structural equation modeling. *Handbook of Psychology, Second Edition*, 2, 2012.

[114] S. United Nations Educational and C. Organization. International Standard Classification of Education (ISCED) 2021.

[115] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying Smartphone User Locking Behavior. In *Proc. SOUPS*, 2013.

[116] VAWnet. Violence against trans and non-binary people.

[117] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, P. G. Kelley, N. Malkin, M. L. Mazurek, M. Sleeper, and K. Thomas. SoK: A Framework for Unifying At-Risk User Research. In *Proc. IEEE S&P*, 2022.

[118] R. Wash and E. Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *SOUPS*, 2015.

[119] M. Wei, P. Emami-Naeini, F. Roesner, and T. Kohno. Skilled or Gullible? Gender Stereotypes Related to Computer Security and Privacy. In *Proc. IEEE S&P*, 2023.

[120] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security*, 1999.

[121] L. Wilcox, R. Shelby, R. Veeraraghavan, O. L. Haimson, G. C. Erickson, M. Turken, and R. Gulotta. Infrastructuring Care: How Trans and Non-Binary People Meet Health and Well-Being Needs through Technology. In *Proc. CHI*, 2023.

[122] S. W. Williams, S. M. Ogletree, W. Woodburn, and P. Raffeld. Gender roles, computer attitudes, and dyadic computer interaction performance in college students. *Sex Roles*, 29(7):515, 1993.

[123] H. Wimberly and L. M. Liebrock. Using fingerprint authentication to reduce system security: An empirical study. *IEEE Security & Privacy*, 2011.

[124] J. O. Wobbrock and J. A. Kientz. Research Contributions in Human-Computer Interaction. *Interactions*, 23(3):38–44, 2016.

[125] R. Zhang, N. N. Bazarova, and M. Reddy. Distress Disclosure across Social Media Platforms during the COVID-19 Pandemic: Untangling the Effects of Platforms, Affordances, and Audiences. In *Proc. CHI*, 2021.

[126] Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proc. CHI*, 2020.

A Literature Review

A.1 Codebooks

We developed three codebooks for our literature review and detail here the topics we coded for, labels within each codebook, as well as definitions and/or examples of each label.

Type of Security Behavior: See Table 2.

Recruitment / Sample Characteristics

- **Representative**: successfully matched sample and population characteristics during recruitment
- **Balanced**: similar number of participants in factor groups for analysis, including work that happened to have balanced samples
- **Limited**: sample characteristics were uncontrolled, e.g., snowball / convenience samples, data collected based on non-sociodemographic criteria and descriptively reports sociodemographic data

Study Methods

- **Self-report**: participants reporting security actions, e.g., interviews conducted in-person or via telephone, surveys
- **Measurement (Observational)**: scraped public data, log data (e.g., from a university, company), or data from software on participants' devices (e.g., mobile app or browser)
- **Measurement (Experimental)**: controlled condition or direct interaction involved, including non-lab study (e.g., MTurk experiment, experiment on social media) or lab study (e.g., in-person, in-lab studies)

A.2 Full List of Papers

Tables 5, 6, and 7 show all papers in our literature review.

B Case Study

B.1 Sociodemographic Factors

We provide here more details on the sociodemographic factors we study in our case study in Section 6. Based on the available log data about Facebook users, we chose six sociodemographic factors to study:

- **Age**, self-reported, bucketed into three groups; 25-34 (46.3%), 35-49 (31.8%), 50+ (21.9%); min: 25, median: 36, mean: 40.14, max: 100
- **Gender**, gender (encoded as binary): women (43.5%), men (56.5%)
- **Educational attainment**, self-reported, scaled per country (e.g., for Brazil, médio incompleto, superior completo, especialização), bucketed into three groups: high school equivalent or less (45.5%), some college (23.6%), BA or higher (30.8%)
- **Geographic location**, one of 16 platform-inferred countries grouped into four regions: *Western* (30.8%): France, Italy, U.S., U.K.; *Latin America* (17.4%): Brazil, Mexico; *Africa and Middle East* (22.4%): Egypt, Kenya, Nigeria, Turkey; *Asia* (29.4%): India, Indonesia, Myanmar, Pakistan, Philippines, Vietnam
- **Internet skill**, measured via Web-Use Skills Index [32, 33], a standardized and validated self-report measure (min: 1.5, median: 3.75, mean: 3.66, max: 5).
- **Technical knowledge**, measured via Pew Research's password knowledge question [70] and three additional questions designed in the same style to assess familiarity with downloads, QR codes, and reacting to posts on the platform of study. Questions ask, "Which of the following best describes" and gives 5 answer options. (Password: 54.1% correct[9]; Download: 61.5% correct; QR: 39.6% correct; Reaction: 46.9% correct)

B.2 Regression Results

Table 8 shows regression results for our case study (see Section 6).

[9] Pew Research [70] found that 75% of U.S. survey respondents answered this question correctly; in our dataset 79.2% of U.S. respondents did so.

Table 5: All 47 papers in our focus dataset, i.e., from our seven selected conferences.

Year	Authors	Title	Conference
2006	Dhamija et al.	Why Phishing Works	CHI
2007	Sheng et al.	Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish	SOUPS
2008	Gilbert et al.	The network in the garden: an empirical analysis of social media in rural life	CHI
2009	Chiasson et al.	Multiple password interference in text passwords and click-based graphical passwords	CCS
	Kumaraguru et al.	School of Phish: A Real-World Evaluation of Anti-Phishing Training	SOUPS
2010	Shay et al.	Encountering stronger password requirements: user attitudes and behaviors	SOUPS
	Sheng et al.	Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions	CHI
	Stutzman et al.	Friends only: examining a privacy-enhancing behavior in Facebook	CHI
2011	Kaye	Self-reported password sharing strategies	CHI
	Sotirakopoulos et al.	On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings	SOUPS
	Wimberly et al.	Using Fingerprint Authentication to Reduce System Security: An Empirical Study	IEEE S&P
2012	Bonneau et al.	The science of guessing: analyzing an anonymized corpus of 70 million passwords	IEEE S&P
	Onarlioglu et al.	Insights into User Behavior in Dealing with Internet Attacks	NDSS
2013	Mazurek et al.	Measuring Password Guessability for an Entire University	CCS
2014	Chen et al.	Exploring Internet Security Perceptions and Practices in Urban Ghana	SOUPS
2015	Ion et al.	"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices	SOUPS
	Jia et al.	Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors	CSCW
	Wash & Rader	Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users	SOUPS
2016	Cho et al.	Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study	CSCW
	Harbach et al.	Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking	CHI
	Redmiles et al.	How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior	CCS
2017	Bonné et al.	Exploring decision making with Android's runtime permission dialogs using in-context surveys	SOUPS
	Fiesler et al.	What (or Who) Is Public?: Privacy Settings and Social Media Content Sharing	CSCW
	Hoyle et al.	Viewing the Viewers: Publishers' Desires and Viewers' Privacy Concerns in Social Networks	CSCW
	Pearman et al.	Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat	CCS
2018	Das et al.	Breaking! A Typology of Security and Privacy News and How It's Shared	CHI
	Machuletz	Webcam Covering as Planned Behavior	CHI
	Redmiles et al.	Examining the Demand for Spam: Who Clicks?	CHI
	Sharif et al.	Predicting Impending Exposure to Malicious Content from User Behavior	CCS
2019	Habib et al.	Impact of Contextual Factors on Snapchat Public Sharing	CHI
2020	Coopamootoo	Usage Patterns of Privacy-Enhancing Technologies	CCS
	Zou et al.	Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices	CHI
2021	Hasan et al.	Your Photo is so Funny that I don't Mind Violating Your Privacy by Sharing it	CHI
	Zhang et al.	Distress Disclosure across Social Media Platforms during the COVID-19 Pandemic	CHI
2023	Bouma-Sims et al.	A US-UK Usability Evaluation of Consent Management Platform Cookie Consent Interface Design on Desktop and Mobile	CHI
	Munyendo et al.	I just stopped using one and started using the other: Motivations Techniques and Challenges When Switching Password Managers	CCS

Table 6: The remaining papers in our full dataset (1999-2014).

Year	Authors	Title	Venue
2004	Milne & Culnan	Strategies for reducing online privacy risks: Why consumers read (or don'tread) online privacy notices	Jrnl. of Interactive Marketing
	Milne et al.	Consumers' Protection of Online Privacy and Identity.	Jrnl. of Consumer Affairs
2005	Youn	Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach	Jrnl. of Broadcasting & E. Media
2007	Grimes et al.	Email end users and spam: relations of gender and age group to attitudes and actions Computers in	Human Behavior
	Jagatic et al.	Social phishing	CACM
	Kumaraguru et al.	Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer	APWG
	Kuo et al.	Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Info. Privacy Practices	Jrnl. of Business Ethics
2008	Bailey et al.	Analysis of Student Vulnerabilities to Phishing.	AMCIS
	Hazari et al.	An Empirical Investigation of Factors Influencing Information Security Behavior	Jrnl. of Info. Privacy & Security
	Lewis et al.	The Taste for Privacy: An Analysis of College Student Privacy Settings inan Online Social Network	Jrnl. of Comp. Mediated Comm.
	Youn & Hall	Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors	Cyber Psychology & Behavior
2009	Dinev et al.	User behaviour towards protective information technologies: the role ofnational cultural differences	Information Systems Journal
	Fogel & Nehmad	Internet social network communities: Risk taking, trust, and privacy concerns	Computers in Human Behavior
	Milne et al.	Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices	Jrnl. of Consumer Affairs
2010	Brandtzæg	Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites	Jrnl. of HCI
	Durand	A Comparative Study of Self-Disclosure in Face-to-Face and Email Communication Between Americans and China	N/A (thesis)
	Hoy & Milne	Gender Differences in Privacy-Related Measures for Young Adult Facebook Users	Jrnl. of Interactive Advertising
	Posey et al.	Proposing the online community self-disclosure model	Euro. Jrnl. of Information Systems
	Siripukdee et al.	Empirical Analysis of Human-related Problems on Information Security in Cross-cultural Environment	Japan Society for Info. & and Mgmt.
	Wright et al.	Where Did They Go Right? Understanding the Deception in Phishing Communications	Group Decision and Negotiation
2011	Kruger et al.	An assessment of the role of cultural factors in information security awareness	Information SecuritySouth Africa
	Lomo-David et al.	University Students Computer Security Practices in Two Developing Nations: A Comparative Analysis	SHSU General Business Conference
	Lowry et al.	Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies	Jrnl. of Management Info. Systems
	Maier et al.	An Assessment of Overt Malicious Activity Manifest in Residential Networks	DIMVA
	Special et al.	Self-disclosure and student satisfaction with Facebook Computers in	Human Behavior
2012	Krasnova et al.	Self-disclosure and Privacy Calculus on Social Networking Sites: The Roleof Culture	BISE
	Madden	Privacy management on social media sites	Pew
	Mohebzada et al.	Phishing in a university community: Two large scale phishing experiments	IIT
	Tufekci	Youth and Privacy in Networked Publics: Active and Complex Engagement	ICWSM
2013	Halevi et al.	A pilot study of cyber security and privacy related behavior and personality traits	WWW
	Litt	Understanding social network site users' privacy tool use Computers in	Human Behavior
	Madden et al.	Teens, Social Media, and Privacy	Pew
	Park	Digital Literacy and Privacy Behavior Online	Communication Research
	Rainie et al.	Anonymity, Privacy, and Security Online	Pew
2014	Alseadoon	The Impact of Users' Characteristics on Their Ability to Detect Phishing Emails	N/A (thesis)
	Baek et al.	My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns	Computers in Human Behavior
	Blank et al.	A New Privacy Paradox: Young People and Privacy on Social Network Sites	ASA

Table 7: The remaining papers in our full dataset (2014-2023).

Year	Authors	Title	Venue
2014	Tembe et al.	Phishing in international waters	HotSoS
	Vanderhoven et al.	How Safe Do Teenagers Behave on Facebook? An Observational Study	PLoS One
2015	Anderson et al.	Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites	Jrnl. of Cybersecurity
	Halevi et al.	Spear-Phishing in the Wild	SSRN
	Marshall et al.	Social networking websites in India and the United States: A cross-national comparison of online privacy and communication	Issues in IS
	Park	Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet	Computers in Human Behavior
	Pattinson et al.	Factors that Influence Information Security Behavior: An Australian Web Based Study	HAS
	Posey et al.	The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets	Jrnl. of Management Information Systems
	Whitty et al.	Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords	Cyber Psychology, Behavior, and Social Networking
2016	Aviv et al.	Analyzing the Impact of Collection Methods and Demographics for Android's Pattern Unlock	USEC
	Bertenthal	Attention and Past Behavior, not Security Knowledge, Modulate Users' Decisions to Login to Insecure Websites	ICS
	Chen & Zahedi	Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China	MIS Quarterly
	Halevi et al.	Cultural and psychological factors in cyber-security II	WAS
	Iuga et al.	Baiting the hook: factors impacting susceptibility to phishing attacks	Human-centric Computing and Info. Sciences
	Kezer et al.	Age differences in privacy attitudes, literacy and privacy management on Facebook	Jrnl. of Psychosocial Research on Cyberspace
	Malik et al.	Privacy and trust in Facebook photo sharing: Age and gender differences	Program
	Petrie et al.	Cultural and Gender Differences in Password Behaviors: Evidence from China, Turkey and the UK	NordiCHI
	Reed et al.	Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures	Social Science Research
	Sonnenschein et al.	Gender Differences in Mobile Users' IT Security Appraisals and Protective Actions: Findings from a Mixed-Method Study	ISIC
	Tsay-Vogel et al.	Social media cultivating perceptions of privacy	New Media & Society
2017	Anwar et al.	The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination	Computers in Human Behavior
	Büchi et al.	Caring is not enough: the importance of Internet skills for online privacy protection	ICS
	Butavicius et al.	Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture	HAISA
	Gavett et al.	Phishing suspiciousness in older and younger adults: The role of executive functioning	PLoS One
	Ifinedo et al.	Effects of Organization Insiders' Self-Control and Relevant Knowledge on Participation in Information Systems Security Deviant Behavior	SIGMIS-CPR
	Sarno et al.	Who are Phishers luring?: A Demographic Analysis of Those Susceptible to Fake Emails	Human Factors and Ergonomics Society
2018	Alohali et al.	Identifying and predicting the factors affecting end-users' risk-taking behavior	Jrnl. of Info. & Comp. Security
	Cain et al.	An exploratory study of cyber hygiene behaviors and knowledge	Jrnl. of Information Security and Applications
	Diaz et al.	Phishing in an Academic Community: A Study of User Susceptibility and Behavior	ArXiV
	Farinosi & Taipale	Who Can See My Stuff? Online Self-Disclosure and Gender Differences on Facebook	OBS
	Griffin	A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks	N/A (thesis)
	Lévesque et al.	Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach	TOPS
	McGill et al.	Gender Differences in Information Security Perceptions and Behaviour	ACIS
	Menard et al.	The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination	Computers & Security
	Millham et al.	Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors	New Media & Society
	Redmiles	Net Benefits: Digital Inequities in Social Capital, Privacy Preservation, and Digital Parenting Practices of U.S. Social Media Users	ICWSM
2019	Dev et al.	Personalized WhatsApp Privacy: Demographic and Cultural Influences on Indian and Saudi Users	SSRN
	Lin et al.	Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content	ToCHI
	Ndibwile et al.	A Demographic Perspective of Smartphone Security and Its Redesigned Notifications	Jrnl. of Information Processing
	Shappie et al.	Personality as a Predictor of Cybersecurity Behavior	Psychology of Popular Media Culture
2019	Tifferet et al.	Gender differences in privacy tendencies on social network sites: A meta-analysis	Computers in Human Behavior
	Breitinger et al.	A survey on smartphone user's security choices, awareness and education	Computers & Security
	Epstein et al.	Markers of Online Privacy Marginalization: Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior	Social Media + Society
	Herbert et al.	Differences in IT Security Behavior and Knowledge of Private Users in Germany	Wirtschaftsinformatik
	Li et al.	Experimental Investigation of Demographic Factors Related to Phishing Susceptibility	HICCS
	Liu et al.	Effects of Demographic Factors on Phishing Victimization in the Workplace	PACIS
	Oghazi et al.	User self-disclosure on social network sites: A cross-cultural study on Facebook's privacy concepts	Jrnl. of Business Research
	Sombatruang et al.	Attributes affecting user decision to adopt a Virtual Private Network (VPN) app	ICICS
	Thao et al.	Human Factors in Homograph Attack Recognition	ANCS
	Zwilling et al.	Cyber Security Awareness, Knowledge and Behavior: A Comparative Study	Jrnl. of Comp. Info. Systems
2021	Abroshan et al.	COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic	IEEE Access
	Abroshan et al.	Phishing Happens Beyond Technology	IEEE Access
	Bhagavatula et al.	What breach? Measuring online awareness of security incidents by studying real-world browsing behavior	EuroUSEC
	Boerman et al.	Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel	Data Comm. Research
	Greitzer et al.	Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility	ACM Transactions on Social Computing
	Grobler et al.	The importance of social identity on password formulations	Personal and Ubi. Comp.
	Kennison et al.	Who creates strong passwords when nudging fails	Computers in Human Behavior
	Mai et al.	Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam	Acta Polytechnica Hungarica
	Morrison	Understanding U.S. Employees' Personality Traits for Phishing Emails Prevention: A Quantitative Study	N/A (thesis)
	Ouytsel	The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships – A mixed-methods study	Telematics and Informatics
	Roberts	Does Digital Native Status Impact End-User Antivirus Usage?	Jrnl. of Comp. Net. & Comm.
2022	Frank et al.	Contextual drivers of employees' phishing susceptibility: Insights from a field study	Decision Support Systems
2023	Du et al.	Phishing: Gender Differences in Email Security Perceptions and Behaviors	Info. Sys. and Comput. Academic Professionals

Table 8: Regression results for the relationships between security behaviors (first row, output variables) and sociodemographic factors and platform metrics (first column, input factors). Each column represents the output of one regression model. Numeric cells list the odds ratio (OR) and the 95% confidence interval. Significance of OR: $p < 0.05$ = *, $p < 0.01$ = **, and $p < 0.001$ = ***. LATAM = Latin America, AME = Africa and Middle East, Edu. = Education, SC = some college, BA+ = Bachelor's degree or more, Tech. = Technical, Know. = Knowledge, L30 = Use (Past 30 days)

	Visit Security Settings	**Action Security Settings**	**Stronger Password**	**Use 2FA**
(Intercept)	0.02*** [0, 0.05]	0.02*** [0, 0.06]	192.25*** [29.13, 1268.55]	0*** [0, 0]
Age (35-49)	0.74* [0.59, 0.94]	0.55*** [0.44, 0.70]	1.18 [0.64, 2.17]	0.79* [0.64, 0.96]
Age (50+)	0.63* [0.42, 0.95]	0.38*** [0.23, 0.63]	2.08* [1.07, 4.03]	0.63* [0.43, 0.92]
Gender (woman)	1.20 [0.97, 1.49]	1.44** [1.14, 1.82]	1.55 [0.86, 2.80]	0.88 [0.73, 1.06]
Location (LATAM)	0.90 [0.56, 1.44]	0.90 [0.53, 1.55]	0.64 [0.20, 2.05]	0.85 [0.42, 1.71]
Location (AME)	0.87 [0.52, 1.46]	0.73 [0.40, 1.35]	0.24* [0.08, 0.71]	1.06 [0.55, 2.03]
Location (Asia)	1.94* [1.15, 3.28]	1.61 [0.87, 2.99]	0.16*** [0.06, 0.45]	1.44 [0.68, 3.02]
Edu. (SC)	1.25 [0.41, 3.79]	1.25 [0.32, 4.77]	0.57 [0.04, 8.41]	7.14** [2.14, 23.85]
Edu. (BA+)	1.36 [0.42, 4.39]	1.39 [0.37, 5.16]	0.89 [0.15, 5.30]	5.40** [1.74, 16.72]
Internet Skill	1.41** [1.12, 1.78]	1.44* [1.09, 1.90]	1.10 [0.79, 1.53]	1.84*** [1.42, 2.39]
Tech. Know. (Download)	1.02 [0.81, 1.29]	0.87 [0.68, 1.11]	0.90 [0.49, 1.65]	0.83 [0.66, 1.04]
Tech. Know. (Password)	0.97 [0.77, 1.23]	1.15 [0.89, 1.49]	1.88* [1.09, 3.23]	1.33* [1.01, 1.74]
Tech. Know. (QR)	1.14 [0.92, 1.42]	1.15 [0.90, 1.47]	1.64 [0.80, 3.36]	1.49*** [1.19, 1.87]
Tech. Know. (Reaction)	1.12 [0.90, 1.39]	1.24 [0.97, 1.58]	1.75* [1.02, 3.00]	1.37** [1.11, 1.70]
Platform Tenure (Years)	0.95** [0.91, 0.99]	0.95* [0.91, 0.99]	0.91* [0.84, 1.00]	1.08*** [1.04, 1.13]
Friends	1.00 [0.99, 1.01]	1.00 [0.99, 1.01]	1.01 [0.98, 1.04]	1.02** [1.00, 1.03]
Use (Past 30 days)	1.00 [0.98, 1.01]	0.99 [0.97, 1.00]	0.97 [0.93, 1.01]	1.01 [0.99, 1.03]
Time Spent	1.01 [1.00, 1.18]	1.03 [0.94, 1.12]	0.90 [0.63, 1.29]	1.13* [1.02, 1.24]
Edu. (SC) * Internet Skill	0.91 [0.68, 1.22]	0.89 [0.63, 1.26]	1.30 [0.65, 2.60]	0.63** [0.47, 0.85]
Edu. (BA+) * Internet Skill	0.88 [0.65, 1.18]	0.85 [0.60, 1.19]	0.92 [0.56, 1.50]	0.71* [0.53, 0.95]
L30 * Time Spent	1.00 [1.00, 1.00]	1.00 [1.00, 1.01]	1.01 [0.99, 1.02]	1.00 [0.99, 1.00]
LATAM * Platform Tenure	1.03 [0.97, 1.10]	1.05 [0.98, 1.12]	0.99 [0.87, 1.14]	0.95 [0.87, 1.03]
AME * Platform Tenure	1.05 [0.99, 1.11]	1.09* [1.02, 1.17]	1.08 [0.96, 1.22]	1.00 [0.94, 1.07]
Asia * Platform Tenure	0.97 [0.91, 1.03]	1.00 [0.93, 1.07]	1.12 [0.99, 1.27]	0.95 [0.88, 1.03]