A Survey of Cybersecurity Professionals' Perceptions and Experiences of Safety and Belonging in the Community

Samantha Katcher, Liana Wang, and Caroline Yang, *Tufts University;*
Chloé Messdaghi, *SustainCyber;* Michelle L. Mazurek, *University of Maryland;*
Marshini Chetty, *University of Chicago;* Kelsey R. Fulton, *Colorado School of Mines;*
Daniel Votipka, *Tufts University*

https://www.usenix.org/conference/soups2024/presentation/katcher

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

A Survey of Cybersecurity Professionals' Perceptions and Experiences of Safety and Belonging in the Community

Samantha Katcher[*▷], Liana Wang[*], Caroline Yang[*], Chloé Messdaghi[‡],
Michelle L. Mazurek[†], Marshini Chetty[◇], Kelsey R. Fulton[∪], and Daniel Votipka[*]
[*]*Tufts University;* [‡]*SustainCyber;* [†]*University of Maryland;*
[◇]*University of Chicago;* [∪]*Colorado School of Mines;* [▷] *MITRE Corporation*

Abstract

The cybersecurity workforce lacks diversity; the field is predominately men and White or Asian, with only 10% identifying as women, Latine, or Black. Previous studies identified access to supportive communities as a possible disparity between marginalized and non-marginalized cybersecurity professional populations and highlighted this support as a key to career success. We focus on these community experiences by conducting a survey of 342 cybersecurity professionals to identify differences in perceptions and experiences of belonging across demographic groups. Our results show a discrepancy between experiences for different gender identities, with women being more likely than men to report instances of harassment and encountering unsupportive environments because of their gender. Psychological safety was low across all demographic groups, meaning participants did not feel comfortable engaging with or speaking up in the community. Based on these result we provide recommendations to community leaders.

1 Introduction

With technology's growing ubiquity, and parallel increases in cyberattacks, skilled cybersecurity professionals are in demand. This demand has outpaced the supply of qualified workers, with some estimates suggesting a four million job shortfall in 2023 [54]. Governments and private institutions are campaigning to increase the number of cybersecurity professionals [8, 35, 36, 51, 85, 110, 113] and the US government has prioritized growing the cybersecurity workforce [7].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

While there have been many efforts to grow the cybersecurity workforce, this growth has not increased diversity. Prior workforce surveys show the field as predominantly male, white or Asian[1], with women, Latine, and Black participants constituting fewer than 10% in each survey [10, 45]. In a 2020 cybersecurity professionals survey, SynAck, a platform connecting organizations with cybersecurity professionals who provide security reviews, found women (66%) and members of marginalized ethnicities (47%) were less likely, when compared to men (88%), to believe people of the same gender or ethnicity were given the same opportunities [102]. Furthermore, interviews with cybersecurity professionals from marginalized populations revealed regular instances of othering, hate, and harassment in the workforce [38].

Cybersecurity's deficiency in diversity creates two problems. First, and foremost, is an equity problem. Members of marginalized populations are driven away from well paying, in-demand careers in cybersecurity. Second, cognitive diversity is essential to secure system design. The more eyes reviewing potentially insecure code, the more thorough a review will be completed and attacks thwarted [63]. People from different genders, ethnicities, and backgrounds provide a fresh perspective to solving complex security problems [28, 69]. As cybersecurity hiring increases, we must prevent furthering existing ethnic and gender disparities by identifying and understanding factors underlying lacking diversity to improve recruitment and retention among marginalized populations.

Recent work investigates the career challenges cybersecurity professionals face through a survey broadly with cybersecurity professionals [2] and interviews with marginalized cybersecurity professionals [38]. Both populations indicated that the most significant challenges were the result of the difficulty of getting started, e.g., navigating unstructured resources to develop necessary skills, and the stress and uncertainty of the market, e.g., trying to find work for which they qualified. Non-marginalized cybersecurity professionals found support

[1]We use the term Asian broadly here, as this is how it is used in the cited prior surveys, but we recognize Asian Americans and those from other regions may still be marginalized in the community.

from their peers crucial, viewing the community as inclusive, while marginalized cybersecurity professionals found it challenging or impossible to join the community, hindering their access to necessary support for success.

In this paper, we take further steps to understand the barriers faced by marginalized cybersecurity professionals by focusing on this point of divergence: their community experiences. We surveyed 342 cybersecurity professionals from varying backgrounds (196 men, 128 women, 10 genderqueer; 215 White, 46 Latine, 38 Black, and 31 other ethnicities). We used multiple validated psychometric scales to measure perceptions of belonging [30, 122] and experiences of supportive and unsupportive social environments [43, 108]. We also asked about participation and experiences in specific subcommunities. We address the following research questions:

- **RQ1:** What differences exist in perception (e.g., belonging, psychological safety) and incidents of unsupportive experiences (e.g., othering, hate, harassment) within the cybersecurity community between marginalized and non-marginalized cybersecurity professionals?
- **RQ2:** Do marginalized and non-marginalized cybersecurity professionals differ in their participation and experiences in specific subcommunities (e.g., work, social organizations, online)?
- **RQ3:** What community interactions are perceived as particularly supportive or unsupportive and how do these differ between marginalized and non-marginalized cybersecurity professionals?

The biggest divide among cybersecurity professionals was across gender identities, with women being more likely to report experiencing harassment and unsupportive environments due to their identity. However, across all demographic groups, cybersecurity professionals reported low psychological safety relative to other professions, indicating the difficultly to engage in the community. Conversely, we did not observe low scores on measures of internal belonging (i.e., whether a participant felt qualified and knowledgable enough to belong in the community). Together these suggest unsupportive forces on cybersecurity professionals are generally external to the individual. Finally, our results suggest early development environments for cybersecurity professionals might be particularly problematic since participants with high school programming experience were less likely to feel psychologically safe. Based on our results, we provide recommendations for cybersecurity community leaders.

2 Related Work

Our study's contribution lies in a focused exploration of belonging in the cybersecurity community, differentiating it from other studies [38, 91, 106, 123]. Here we describe prior work and how our study fits into the broader research context.

Marginalized populations' experiences in computer science and technology. There is a growing body of research considering issues facing marginalized populations in CS and STEM domains. For example, work studying developers has found marginalized populations are paid less [42, 73] and are less likely to have work accepted by colleagues [9, 74, 105, 116]. Similarly, significant research has investigated issues in CS [16, 17, 18, 34, 64, 65, 92, 95, 123] and technology careers more broadly [14, 86, 124]. Margolis and Allen performed an ethnographic study of the gender gap in CS education [65]. They found women had less coding experience than men in undergraduate programs and perceived CS's "geek" culture negatively. Subsequent work has documented issues of gendered perceptions of CS [15, 22, 72, 76, 93], which are further entrenched by unapproachable early educational activities [3, 19, 60] , lack of representation [3, 109], mentorship support [1, 3, 19, 109, 126], and a non-inclusive culture to diverse backgrounds and experiences [1]. Because we expect many of these trends to be mirrored in cybersecurity, we use this prior work as a lens, guiding our survey questions and analysis. However, we expect cybersecurity may present differences as it is more specialized and the inherent focus on privacy and security scrutiny may make cybersecurity communities less welcoming. This has been found, to some extent, demonstrating several differences in interviewee experiences when studying members of the vulnerability discovery community—a subset of the cybersecurity community [38].

Marginalized populations' experiences in cybersecurity. Several prior industry surveys have demonstrated the lack of diversity in the cybersecurity community [10, 44, 54, 102]. This includes ICS2's annual survey of the cybersecurity workforce, which showed that the younger generation (under 30 years old) of cybersecurity professionals are more diverse. However, this diversity remains limited as only 26% of this generation are women [54]. This survey also found the pathways into cybersecurity differ by gender and race/ethnicity. Women and non-white cybersecurity professionals are more likely to come from a traditional education-based pathway (e.g. college) and less likely to come from an IT background.

In addition to these industry surveys, some academic interview-based studies have examined the challenges marginalized cybersecurity professionals face [38, 83, 91, 106, 112]. Fulton et al. conducted semi-structured interviews with members of the vulnerability discovery community from marginalized populations, uncovering challenges specific to members of marginalized populations, such as a difficulty being taken seriously by others, a reluctance from other community members to share information, and explicit discrimination within the community. Additionally, Fulton et al's works discussed the important role mentors played in participants' experiences [38]. In interviews with 21 cybersecurity

professionals, Schoenmaker et al. found some participants believed holding a minority status might cause an increase in an individual's ability to monitor for security anomalies, as these individuals already have significant experience monitoring for threats regarding personal safety. However, they also observed social conventions and lack of access to resources might make it more difficult for these groups to practice vulnerability discovery [91]. Plato et al. interviewed sixteen women C-Suite executives in cybersecurity to learn about their journeys into leadership and experiences with mentorship, sponsorship, and trusted advisors, as well as experiences of biases and discrimination highlighting how networking, mentorship, and observing leadership styles play pivotal roles in shaping individuals' trajectories, even with a shortage of female mentors and racial bias making this difficult to accomplish in practice [83]. Each of these studies highlights important challenges marginalized cybersecurity professionals face, but have limited generalizability due to their small samples. Our work expands on these findings with a large-scale survey focusing on community belonging, a central challenge observed in prior work.

Students' cybersecurity experiences. Some work has investigated existing workforce disparities. This work has primarily focused on student experiences in security exercises [29, 84] and college courses [13] as students take the first steps toward cybersecurity careers. It provides some indications of students' reasons for abandoning the field (e.g., lack of role models and community, gendered stereotypes) and suggests entry-level hands-on exercises can increase interest. While these education-focused questions are important, cybersecurity professionals face challenges throughout their careers [38] and prior work has found many are not trained through these traditional educational settings [45, 121]. To address this gap, our work takes a holistic view of cybersecurity professionals' community environments.

3 Methods

We seek to understand how practitioners in cybersecurity participate in and perceive belonging within their professional community, and specifically to consider differences and similarities between practitioners from different demographics. We do not place limits on participation (e.g., industry, academia, government), but consider the field of cybersecurity broadly. In this section, we describe the survey design, recruitment methods, data analysis procedures, ethical considerations, and the work's limitations.

3.1 Survey Design

The survey began by requesting participant consent; included three main components aligned with the research questions; and concluded with demographics questions. Figure 1 summarizes the survey's flow. The full survey can be found in Appendix A. Where applicable, we altered validated scales to focus on cybersecurity and the cybersecurity community, and we included attention checks to catch inattentive respondents [68]. The survey was divided into three parts to match our research questions: questions about participants' belonging within the cybersecurity community generally (RQ1), participation in various subcommunities–listed in Table 2–(RQ2), and prototypical community experiences (RQ3). We detail how we asked about each of this topics in turn, then concluded with questions about their security experience and demographics. Figure 1 summarizes the survey's flow. Participants completed the survey in 15 minutes on average.

Perceptions of belonging (RQ1, Figure 1.B). We first sought to understand whether participants feel they belong in the cybersecurity community, as prior work found cybersecurity professionals were more successful after finding a community where they could get support and ask questions [38].

We utilized three validated psychometric measures of belonging: *psychological safety* [30], *belonging uncertainty* [122] and *vulnerability discovery self-efficacy* [119]. Table 1 provides additional details about each scale.

The psychological safety scale has previously been used to investigate why employees feel comfortable sharing information [21, 94], suggesting organizational improvements [27, 62], and taking initiative [5]. The belonging uncertainty scale has predominately been used investigate feelings of otherness among historically underrepresented groups, for example, among professionals [122] and students [26]. We also ask participants explicitly whether people with similar backgrounds have opportunities to participate in cybersecurity work to assess the question of representation more directly.

Finally, to assess whether participants believed they had the skill to be in the community (i.e., separate from whether they believed others would accept them into the community) we used the vulnerability discovery sub-scale of Votipka et al.'s secure software development self-efficacy scale (SSD-SES), which asks participants to assess their proficiency to identify vulnerabilities [119]. SSD-SES has been used to assess differences in perceived ability between study subgroups [56, 103, 104] and as a measure of learning improvement with educational interventions [39, 120].

(Un)welcoming Community Experiences (RQ1, Figure 1.B). To understand concrete experiences that might impact cybersecurity professionals' community participation, we asked a modified version of de Grey et al.'s Online Social Experiences Measure (OSEM), which assesses social support and negativity arising from online social network interactions [43]. OSEM evaluates aspects such as emotional, informational, and instrumental support. This measure has been employed in research to understand how online interactions influence mental health and social well-being, particularly in

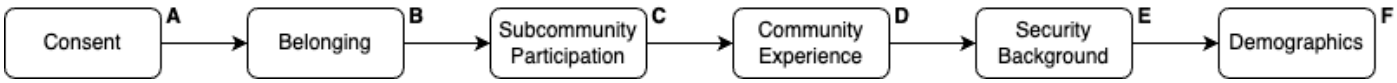


Figure 1: Structure of the survey.

Name	Description	Ex. Item	Response Opts.	Items	Agg[1]
Psychological Safety [30]	whether participants feel safe to express themselves, take risks, and ask questions	"If you make a mistake in the cybersecurity community, it is often held against you"	7-pt; "Very inaccurate" to "Very accurate"	5	Avg
Belonging Uncertainty [122]	Whether participants feel people like them belong in the community	"When something bad happens, I feel that maybe I don't belong in cybersecurity"	7-pt; "Strongly disagree" to "Strongly agree"	3	Avg
Vuln Discovery Self-Efficacy [119]	Whether participants believe they have appropriate cybersecurity skills	"I can identify potential security threats to the system"	5-pt; "Not confident at all" to Absolutely confident"	9	Sum
Online Social Experiences [43]	How often participants experience positive and negative interactions	"Someone in the cybersecurity community has made me feel embarrassed or foolish"	5-pt; "Very Slightly or Not at All" to "Extremely"	8	Sum
Hate and Harassment [108, 117]	How often participants experience hate and harassment	"Stereotyping based on perceived demographic characteristics"	4-pt; "Never" to "Frequently"	7	Sum

[1]Aggregation function used to combine responses from multiple items to a single score.

Table 1: Summary of psychometric measures used in the survey to understand participants' sense of belonging and experiences in the cybersecurity community. The different scales were presented in a randomized order to avoid ordering effects.

digital communities [20, 75, 111].

To capture hate and harassment, we borrowed from Thomas et al.'s [108] and the Pew Research Center's [117] existing survey questions investigating online hate and harassment. We included four questions about severe negative experiences which OSEM did not include, namely stereotype bias, violence, sexual advances, and doxxing. These questions have been employed in various research contexts to measure experiences of sexual harassment, particularly in professional and educational settings [24, 57, 81].

Subcommunity participation (RQ2, Figure 1.C). Community is not a global construct, but instead is specific to the individual [90]. Someone might not feel comfortable communicating with others at a large security conference, but may establish a smaller local community where they feel strong connections and receive support. Therefore, we investigated how participants' experiences varied across subcommunities–specifically, those descried in Table 2, drawn from prior work [38]. We asked how many of each type of subcommunity participants were members of, how frequently they discussed cybersecurity concepts and how helpful they found each subcommunity, and, for each subcommunity, we asked at least one subcommunity-specific question to allow a better understanding of participant's relationship to the subcommunity. We randomized the order participants were asked about each subcommunity to avoid ordering effects.

Examples of supportive and unsupportive community experiences (RQ3, Figure 1.D). Next, we sought to understand what makes participants feel particularly welcome or unwelcome. We asked participants to describe an experience where they felt particularly well supported which could involve explicit assistance, encouragement, or any positive influence that aided the participant's professional growth. We also asked participants to describe a particularly unsupportive experience, which could include instances where the interaction was harmful or hindered their professional progress.

Cybersecurity background and demographics (Figure 1.D/E. We finished by asking about participants' cybersecurity background, i.e., the extent their work focuses on cybersecurity, whether and what kind of cybersecurity training they have received, when they began programming, the age they became interested in cybersecurity, and the age they first received cybersecurity career support. We ended with demographics questions like gender, ethnicity, and education.

3.2 Recruitment

Recruiting cybersecurity professionals is a difficult task because they are a small, well paid population with significant demands on their time [47, 59]. Our challenge was compounded by the fact that we weighted our sample toward marginalized cybersecurity professionals, who make up a small fraction of this small workforce [10, 45].

We used several recruit methods, including contacting cybersecurity professional organizations' leaders; advertising in

Subcommunity	Description
Close Friends / Mentors	Family, friends and other close mentors who provided either career or other support (e.g., emotional, economical, etc.)
School	A learning community focused on cybersecurity in an academic setting (e.g., class, student-run organization)
Work	Community in participants' workplaces where they are able to discuss cybersecurity topics and receive support
Organizations	Groups outside work and school (e.g., ACM chapters, Women in Security and Privacy)
Online and Conferences	The broader cybersecurity community where participants might meet and talk with other, but not have close or lasting relationships. This includes interactions at cybersecurity conferences or workshops, as well as through online forums (e.g., StackOverflow, Reddit, X (formerly Twitter), public Slack or Discord).

Table 2: Types of subcommunities participants were asked about.

Factor	Description	Baseline
Required		
Gender	Gender participants identify as	Man
Ethnicity	Ethnicity participants identify as	White
Optional		
Yrs. Exp.	Number of years participants have worked in cybersecurity	–
Yrs. Until Mentor	Age when participant first had a mentor who helped them learn about cybersecurity	–
Helpful Mentor	Whether participant reported having someone close (mentor/family member/friend) who helped them learn about cybersecurity	False
HS Prog.	Whether participant had high school programming experience	False
Job/ Seniority	Current job role (junior, senior non-leadership, senior leadership, or not currently working in cybersecurity)	Junior

Table 3: Factors used in regression models. Categorical variables are compared individually to the baseline.

public (i.e., X (formerly Twitter), LinkedIn, and Reddit) and private (i.e., Slack and Whatsapp) online spaces; recruiting at cybersecurity conferences; and contracting Qualtrics for a curated panel. Participants recruited through organizations, online, and conferences were given a study description and entered into a raffle for one of 25 $50 Amazon gift cards. For the Qualtrics panel, we instructed Qualtrics to identify paenlists working in cybersecurity, with a majority being women and at least 30% non-white. Panelists were paid $25.

Our recruitment messages indicated that anyone currently working (or having worked in the last two years) in cybersecurity could participate. We did not mention the study's intent to compare responses between marginalized and non-marginalized cybersecurity professionals to avoid a potential backlash [55, 88] due to increasing antagonism and polarization around diversity, equity, and inclusion efforts from a segment of the population [32, 70].

3.3 Data Analysis

Next, we outline our quantitative and qualitative analyses.

Qualitative analysis. To analyze the two free response questions in Part C, we used iterative open coding [100]. Two researchers collaboratively reviewed the first 35 responses to generate the codebook. Then, the same two researchers iteratively coded responses in rounds of twenty. After each round, the coders compared responses, resolved disagreements, and updated the codebook as necessary. After six rounds of independent coding (i.e., 120 responses), the coders achieved a Krippendorff's α of 0.858 for *what* participants experienced and 0.835 for *who* the experience was with. Both are above the recommended level of agreement [46]. The remaining responses were divided evenly among the coders and coded independently. The final codebook is included in the supplemental materials [101].

Quantitative analysis. In our statistical tests, we limited our dataset to participants who identified as men or women and were White, Black, and/or Latine. We did not include other demographics for statistical tests because there was an insufficient number of participants to produce generalizable results. We include 289 participants in the reported statistical anlaysis.

For the vulnerability discovery self-efficacy, online social experiences, and harassment questions, we used a poisson regression as the scales were scored using a sum of the Likert responses. As the harassment questions from Thomas et al. are not part of a validated scale, we first computed Cronbach's α over participants' responses to the four harassment questions to test their internal consistency [67]. These questions had "good" internal consistency ($\alpha = 0.806$), so we chose to treat them as a single measure like the other scales. For the psychological safety and belonging uncertainty scales, we used linear regressions as the outcome variables were a percentage and an average, respectively. To generate our initial models, we included all the factors listed in Table 3. Because it is possible some explanatory variables are not independent, which would violate the regressions' assumptions [12, pg. 67-106], we tested for multicollinearity and found there was no significant correlation between factors. We then conducted model selection on all possible combinations of these factors, only considering models that included gender and ethnicity as they were our key variables of interest and selected the model with minimum Bayesian Information Criteria (BIC) [87, 96].

For each subcommunity, we used Kruskal-Wallis H tests,

to compare subcommunity membership, discussion participation rates, and helpfulness Likert responses. We began each comparison with an omnibus test over all demographic groups. If the result was statistically significant, we applied planned pairwise comparisons between non-marginalized and marginalized groups for gender and ethnicity, i.e., men to women, White to Black, White to Latine.

Finally, we applied Pearson's χ^2 tests to compare responses between top-level code categories between men and women for themes that were mentioned by at least five participants [37] for our free-response questions. We focused on gender differences as we do not have sufficient data points across races/ethnicities to produce generalizable results. For categories mentioned by five or fewer of a single gender group, we perform a Fisher's Exact Test instead of a χ^2 test [33].

3.4 Ethical Considerations

This study was approved by our institution's ethical review board. Since this survey asks about multiple sensitive topics including experiences of harassment, psychological safety, and social experiences, participants were informed about our data collection and secure storage practices and that they could stop participating or skip a question at any time.

3.5 Limitations

Our study has several limitations that should be considered when interpreting our results.

Self-report responses. As is common in online studies with self-reported data, some participants may not approach the survey seriously, may try to take the survey multiple times, or may fabricate responses to qualify for compensation. To account for these behaviors, we deterred multiple responses by using a browser cookie and followed best practices for removing inattentive responses, e.g., we removed those that failed attention checks, were significantly faster than average, or provided nonsensical responses to open-ended questions (N=385). Also, we received over 500 automated responses where more than 50 identical or nearly identical responses were submitted within a very short period–often within a minute. We removed these responses as they were received as they clearly did not represent a legitimate response.

Inauthentic responses were a challenge in this study. To mitigate this, we primarily recruited from venues with a high likelihood of cybersecurity professionals, leveraging community relationships and in-person recruiting. Qualtrics panel participants were recruited independently of our study, reducing their motivation to lie, and their open-ended responses were consistent with those from professional venues.

Demographic distribution and US-centric population. While we made significant efforts to recruit participants from marginalized populations, many identities have limited representation in our sample (e.g., genderqueer, Middle Eastern, indigenous peoples). Therefore, any results from their responses may not generalize beyond our sample. We give descriptive statistics regarding their responses to provide indications of potential trends for future work to investigate, but avoid conducting statistical tests relating to these identities or making broader statements about their responses. Similarly, our small sample sizes preclude investigation into the effects of intersectional identities. We expect there are important differences introduced by intersectionality, as prior work has shown in other domains [78, 97], but we refrain from investigating them to avoid overgeneralizing their personal experiences.

Despite attempting to recruit broadly, our participant pool was predominantly US-centric, with 279 out of 342 respondents from the US. We expect experiences of cybersecurity professionals in other regions will be similar, but there are likely critically important differences; we encourage further work focus on other geographic areas.

Survivor and recall biases. Our recruitment was limited to currently or recently employed cybersecurity professionals. It is likely many members of marginalized populations considered becoming cybersecurity professionals or worked in the field, but faced substantial challenges and chose to switch professions. Our results inherently do not account for these individuals, so our findings may skew toward a more positive portrayal of cybersecuirty. We attempt to capture some of this adversity by asking participants to consider their experiences throughout their career when answering all questions, but they may not clearly remember events from years ago [89].

Demand effects. Participants might be motivated to report more or less unsupportive experiences based on political or cultural views or other social factors. Some participants from marginalized populations might under-report unsupportive experiences to avoid being seen as "whining" or as not earning their success [41, 98]. Alternatively, non-marginalized participants might over-report unsupportive experiences to counter what they see as "woke" popular perceptions [32, 55, 70]. To identify these biases, we include multiple community inclusivity measures and open-ended questions to capture participants' experiences from multiple vantage points. However, these effects likely narrow any differences we might identify between non-marginalized and marginalized populations.

3.6 Positionality Statement

We acknowledge our identities can significantly influence research process and outcomes [6, 48]. Our research team is diverse, comprising three Asian women, three White women (two Jewish), one White nonbinary person, and one White man. The team includes four professional academics who teach security courses, five cybersecurity professionals, four members with government service experience, and two under-

graduate students. All currently reside in the United States. Our overlapping identities as researchers and our personal experiences have led us to observe instances of unwelcoming and unsafe environments in the field of computer security and privacy, as well as instances of harassment in the community.

4 Participants

Table 4 provides a summary of our 342 participants' demographics, divided by gender and race/ethnicity. Most of our participants identified as men (57%) or women (37%). The vast majority of our participants identified as either White or of European descent (63%), Black or of African descent (11%), and/or Hispanic or Latine (13%). Our participants were mostly located in the US (N=279).

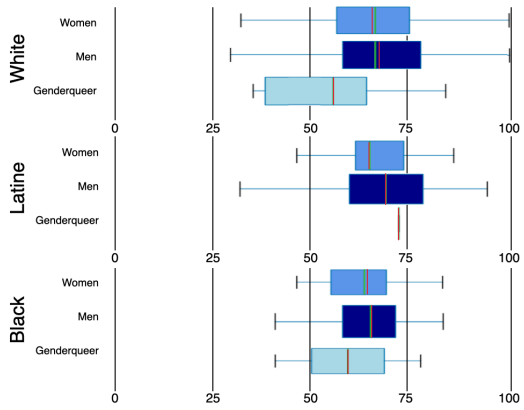
The majority of our participants reported having taken at least one programming course in high school (N=234). On average, participants reported 7.5 years of security experience and had job titles including leadership positions, managerial roles, technical positions, and specialized roles related to security analysis and engineering, even holding more senior roles (N=178), such as 'Senior Security Officer" or "CISO". Our participants' had a wide-range of job roles (e.g malware analysis, secure development, and SOC operations).

5 Perceptions of Belonging and Social Experiences (RQ1)

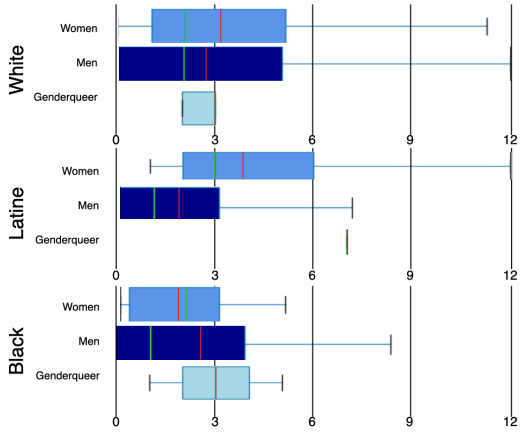
We found few differences in responses between demographics. However, we observed widespread low perceptions of belonging and that women were more likely to experience more severe forms of hate and harassment.

Psychological safety is low for everyone. We observed low psychological safety for all participants: 65.5 on average, which falls into the bottom quartile of scores from a cross-industry benchmark [40]. However, our participants' average belonging uncertainty was lower (indicating less uncertainty) than samples from prior work, which showed higher uncertainty for both non-marginalized and marginalized groups of professionals [122] and students [26]. This suggests our participants overall feel they belong in cybersecurity, but do not feel comfortable speaking up in the community.

No observed differences in perceptions of belonging between genders or races/ethnicities. When comparing psychological safety and belonging among genders the average scores for men (psychological safety 66.6, belonging uncertainty 14.2), women (64.6, 14.3), and genderqueer (60.0, 13.1)were similar. White participants (65.7, 14.2) reported similar scores as participants who identified as Black (64.5, 13.7) or Latine (67.4, 14.6). The similarities across demographic groups can be seen in Figure 2a and Figure 2, which



(a) Psychological safety scores across gender and ethnicity



(b) Severe harassment scores across gender and ethnicity

Figure 2: Quantitative results from survey questions about perceptions of belonging and social experiences. The green line indicates the median and the red line indicates the mean for each metric.

plot participants' psychological safety and belonging scores, grouped by gender and race/ethnicity.

The psychological safety regression (Table 5a) found no statistically significant correlation for gender or race/ethnicity. Psychological safety was negatively correlated with participants who reported taking a programming course in high school. Participants who took high school programming scored 5.9 points lower on average while controlling for other factors ($p < 0.001$), indicating participants who began developing cybersecurity skills earlier feel less safe in the community. The final model for belonging uncertainty did not explain a significant variance ($R^2 < 0.02$), so we do not provide it here or discuss it further.

Severe harassment more common for women and those who enter the field earlier. Focusing specifically on severe instances of negative social experiences, namely violence, stereotyping, doxxing, and sexual advances, Figure 2b shows the distribution of severe harassment responses, organized by gender and races/ethnicities. Overall, we note that severe harassment is rare. The average score was 3 out

	Men	Women	Genderqueer	White	Black	Latine	Total
Men	**196 (57%)**	-	-	125 (37%)	22 (6%)	28 (8%)	196 (57%)
Women	-	**128 (37%)**	-	83 (24%)	14 (4%)	17 (5%)	128 (37%)
Genderqueer	-	-	**10 (3%)**	5 (2%)	2 (1%)	1 (0.3%)	10 (3%)
No Answer	-	-	8 (2%)	-	-	-	8 (2%)
White	125 (37%)	83 (24%)	5 (2%)	**215 (63%)**	-	-	215 (63%)
Black	22 (64%)	14 (4%)	2 (1%)	-	**38 (11%)**	-	38 (11%)
Latine	28 (8%)	17 (5%)	1 (0.3%)	-	-	**46 (13%)**	46 (13%)
Avg. Yrs in Sec.	8.3	6.6	5.1	8.1	6.8	8.1	7.5
Heterosexual	169 (49%)	110 (32%)	2 (1%)	186 (54%)	32 (9%)	40 (12%)	291 (85%)
Gay/Lesbian	4 (1%)	3 (1%)	1 (0.3%)	6 (2%)	1 (0.3%)	1 (0.3%)	8 (2%)
Bisexual	8 (2%)	11 (3%)	3 (1%)	12 (4%)	5 (2%)	4 (1%)	24 (7%)
High school	12 (4%)	7 (2%)	0 (0%)	11 (3%)	3 (1%)	2 (1%)	19 (6%)
Some college	15 (4%)	14 (4%)	1 (0.3%)	17 (5%)	5 (2%)	8 (2%)	30 (9%)
Associate degree	12 (4%)	15 (4%)	0 (0%)	21 (6%)	3 (1%)	2 (1%)	27 (8%)
Bachelor's degree	72 (21%)	45 (13%)	5 (2%)	77 (23%)	12 (4%)	22 (6%)	122 (36%)
Master's degree	63 (18%)	39 (11%)	3 (1%)	71 (20%)	14 (4%)	12 (4%)	105 (31%)
Doctorate	14 (4%)	5 (2%)	0 (0%)	17 (5%)	1 (0.3%)	0 (0%)	19 (6%)
Junior role	79 (23%)	43 (13%)	3 (1%)	79 (23%)	13 (4%)	20 (6%)	131 (38%)
Senior role	73 (21%)	55 (16%)	4 (1%)	90 (26%)	18 (5%)	17 (5%)	132 (39%)
Senior leadership	30 (9%)	18 (5%)	0 (0%)	34 (10%)	7 (2%)	8 (2%)	48 (14%)

Table 4: Participant demographics divided by gender identity and race/ethnicity. For each cell we provide the number of participants, as well as the percentage of the total participant pool. Note, we only include the top three most common races/ethnicities and participants could mark multiple races/ethnicities, so those numbers will not sum to 100%. Additionally, two participants self-described their gender identities.

of a possible 12 points and a majority of participants reported "Never" experiencing violence (69.0%), sexual advances (62.0%), or doxxing (60.5%). The exception regarded experiences of stereotype bias, which participants most often reported "Never" experiencing (32.5%), but a non-trivial number reported experiencing it "Rarely" (29.5%), "Occasionally" (25.4%), or Frequently (12.6%).

Women and genderqueer participants reported more frequent occurrences of severe harassment (average frequency scores 3.2 and 3.7 out of 12, respectively) than men (average 2.8). Table 5b shows this correlation was statistically significant ($LE = 1.2, p = 0.015$), indicating women were $1.2\times$ more likely to report more frequent severe harassment than men.We did not observe a similar statistically significant difference for race/ethnicity.

Again, we observed that high school programming experience correlated with an increase in negative outcomes for participants. Participants with high school programming experience were an estimated $1.6\times$ more likely to report severe harassment ($p < 0.001$). We also found participants with more security experience were slightly less likely to report experiences of severe harassment ($LE = 0.9$, $p = 0.016$).

No observed statistically significant difference in social experiences. We did not observe any statistically significant differences between genders or races/ethnicities on the OSEM scale. Men's (17.9) and women's (17.4) average scores were similar, however genderqueer participants' scores were slightly higher (21.9), indicating a higher rate of unsupportive experiences. Also, White participants (18.2) reported similar OSEM scores as Black (17.4) or Latine (16.6) participants. The regression over OSEM scores is summarized in in the supplemental materials [101]. The only statistically significant correlation was for participants with a helpful close relationship who were expected to have OSEM scores $0.8\times$ participants' without close relationships ($p < 0.001$). Because this LE is < 1, this indicates a lower score and less negative experiences, as close relationships likely provide important support.

White security experts have lower vulnerability discovery self-efficacy. On average, White participants reported statistically significantly lower vulnerability discovery self-efficacy (32.8) than Black participants (36.6). White participants' scores are estimated to be $0.9\times$ Black participants' scores, holding all other factors equal ($p < 0.001$), as seen in Table 6. We did not see a similar difference between Black and Latine participants. We did not see the same stark differences for gender. On average, men's scores on the vulnerability discovery self-efficacy metric were slightly higher (34.2) than women's (33.0) and genderqueer participants, but gender does not appear in our final regression model.

Security experts with more experience have higher vulnerability discovery self-efficacy. Participants who have left the field or have yet to enter the workforce had lower scores than

Variable	Value	Coef	CI	p
Gender	Man	–	–	–
	Woman	-2.3	[-5.6, 0.9]	0.170
HS Prog	False	–	–	–
	True	**-5.9**	**[-9.4, -2.4]**	**0.001***

– Base case (Coef=0, by definition)
*Significant effect

(a) Psychological safety linear regression.

Variable	Value	LE	CI	p
Gender	Man	–	–	–
	Woman	**1.2**	**[1.6, 3.0]**	**0.015***
Sec Yrs	–	**0.9**	**[0.9, 1.0]**	**0.016***
HS Prog	False	–	–	–
	True	**1.6**	**[1.2, 2.1]**	**<0.001***

– Base case (Log Estimate(LE)=1, by definition)
*Significant effect

(b) Severe harassment Poisson regression.

Table 5: Summary of regression over participant psychological safety (A) and severe harassment (B). R^2 for the psychological safety model was 0.04 and the Pseudo R^2 for the harassment model was 0.06 (corrected Aldrich-Nelson).

those currently working in security ($LE = 0.9$, $p = 0.020$). Participants in more senior ($LE = 1.1$, $p < 0.001$) or C-Suite ($LE = 1.2$, $p < 0.001$) roles reported higher vulnerability discovery self-efficacy than participants in junior roles. Similarly, participants with earlier exposure to programming reported $1.1\times$ higher vulnerability discovery self-efficacy than participants who began programming later ($p = 0.002$). Also, we observed participants who reported having close helpful relationships had statistically significantly higher vulnerability discovery self-efficacy ($LE = 1.1$, $p = 0.012$), echoing the benefits of having a mentor from prior work [38].

6 Subcommunity Participation (RQ2)

Next, we turn to participants' reported subcommunity experiences. Figures 3 and 4 show participants' reported membership in and perception of helpfulness, respectively, for each subcommunity, divided by demographic group. For brevity, we show reported rate of discussion in the supplemental materials [101], as there were no clear differences between groups.

No difference in subcommunity membership or rate of discussion. Participants most often reported discussing security at work (57.3%), having close friends/mentors (56.7%), joining learning communities while in school (48.2%), and participating in online forums or conferences (37.1%). We did not observe a statistically significant difference in subcommunity membership or discussion rates for any demographic groups. Participants who reported joining each subcommunity most often reported discussing security occasionally (54.8% - close friend/mentors, 51.1% - online and conferences, 47.3% - organizations) or frequently (51.7% - work, 40.1% - school).

Variable	Value	LE	CI	p
Ethnicity	Black	–	–	–
	Latine	0.9	[0.9,1.0]	0.364
	White	**0.9**	**[0.8,0.9]**	**<0.001***
Close Helpful	False	–	–	–
	True	**1.1**	**[1.0, 1.1]**	**0.011***
HS Prog	False	–	–	–
	True	**1.1**	**[1.0, 1.1]**	**0.002***
Role	Junior	–	–	
	Not in Sec	**0.9**	**[0.7, 1.1]**	**0.020***
	Senior	**1.1**	**[1.1, 1.2]**	**<0.001***
	C-Suite	**1.2**	**[1.1, 1.2]**	**<0.001***

– Base case (Log Estimate (LE)=1, by definition)
*Significant effect

Table 6: Summary of regression over participant vulnerability discovery self-efficacy scores. The Pseudo R^2 (corrected Aldrich-Nelson) for the self-efficacy model was 0.25.

Women prioritized identity-focused organizations. Focusing specifically on the types of organizations participants reported being members of, we observed a significant difference between women and men. Women (39.8%) were statistically more likely than men (14.8%) to join "identity-focused" organizations ($\chi^2 = 18.3, p < 0.001$), such as Women in Cybersecurity. However, these rates flipped for general-focus organizations, as men more often joined these groups (59.7%) than women (38.3%), and this difference was statistically significant ($\chi^2 = 6.6, p = 0.010$). We did not observe a similar divide between races/ethnicities for either identity-focused ($\chi^2 = 2.5, p = 0.284$) or general-focus ($\chi^2 = 0.2, p = 0.917$) organizations. We did not observe a similar trend among genderqueer participants as four (of ten) reported membership in identity-focused organizations and four were members of general-focus organizations.

Black participants found community organizations more helpful than White participants. A majority of both Black and White participants who were members of community organizations perceived them as helpful. However, Black participants skewed significantly ($\chi^2 = 5.5, p = 0.019$) more positive regarding community organizations (74.2% extremely helpful, 22.6% somewhat helpful) than White participants (51.3% extremely helpful, 40.3% somewhat helpful).

7 Supportive and Unsupportive Experiences (RQ3)

Finally, we turn to participants' reports of (un)supportive experiences within the cybersecurity community. 307 of the 342 participants responded: 301 described supportive experiences (88.0%) and 291 described unsupportive experiences (85.1%).

We note that a lack of response does not necessarily indicate a lack of supportive or unsupportive experiences, as

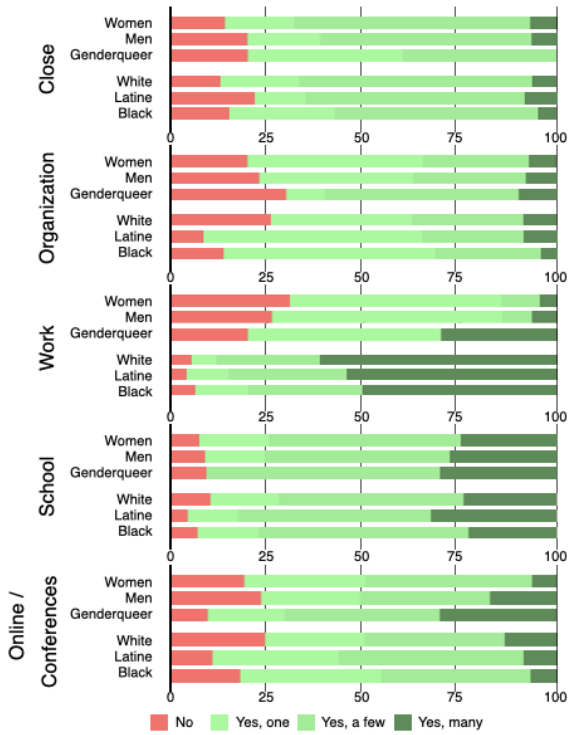


Figure 3: Subcommunity membership grouped by gender and race/ethnicity.

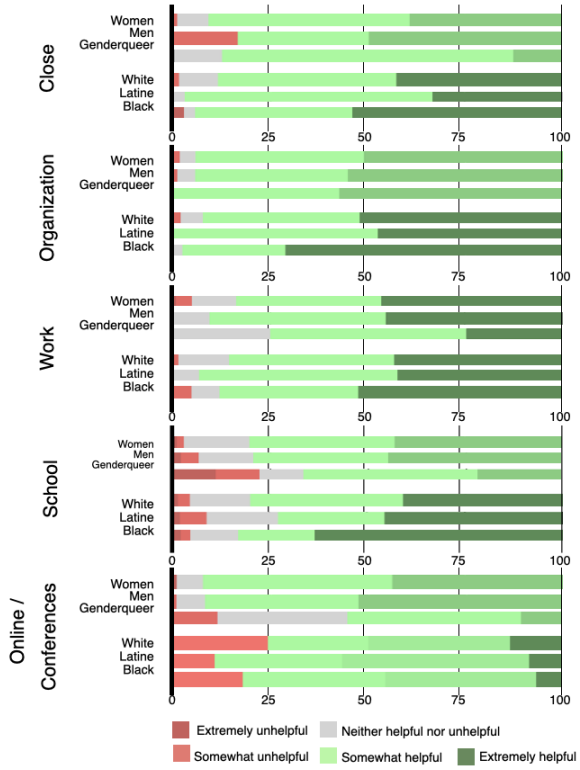


Figure 4: Community helpfulness grouped by gender and race/ethnicity.

	Men	Women	Genderqueer	Total
White	106 / 101	72 / 73	3 / 3	183 / 179
Black	23 / 21	18 / 18	2 / 2	43 / 41
Latine	25 / 24	17 / 16	1 / 1	43 / 41
Total	172 / 163	115 / 114	7 / 7	301 / 291

Table 7: Participant demographics divided by gender and ethnicity for participants who provided examples of supportive (first number) and unsupportive (second number) community experiences.

responding to these questions was optional. Our analysis focuses on trends observed between men and women, as responses from other genders and races/ethnicities were limited. We did not observe clear differences in the percentages of reported supportive and unsupportive experiences across race/ethnicity, so we do not report those numbers for brevity. However, this should not preclude future work from achieving higher recruitment across these demographics.

Women experienced more unsupportive, negative identity-based incidents. Women (N=14, 12.3%) were significantly ($\chi^2 = 5.18$, $p = 0.023$) more likely to describe encountering an unsupportive environment than men (N=9, 5.5%). For example, one woman shared, "I had a project with a colleague who is not anywhere near as technical as I am, yet he consistently tried to micromanage my technical work, and sometimes told me I was doing things wrong even though he didn't know what he was talking about." When men reported unsupportive environments, these were often due to differing goals or personalities, unlike the devaluation of skills observed with women. For example, one man stated, "[I have been] able to hop projects and or jobs in the past when I felt a workplace was not supportive of the direction I wanted to grow in... Once to avoid policies, and once to avoid a person I did not work with well." Men often reported being able to navigate out of these unsupportive environments relatively easily.

Women (N=16, 14.0%) reported significantly ($\chi^2 = 5.2$, $p = 0.023$) more negative experiences related to their identity than men (N=10, 6.1%). One woman explained, "I was at a career fair and the person at the booth refused to talk to me. They ignored me ... as I patiently waited and proceeded to talk to people who showed up after me... All while refusing to acknowledge my presence. I figure it had something to do with the fact that I was the only female at the booth."

Men more often reported never having an unsupportive experience. Some participants explicitly said they had no supportive (N=10, 3.3%) or unsupportive experiences (N=97, 33.3%). Men were more likely not to have unsupportive experiences (N=59, 36.2%) than women (N=36, 31.6%), though the difference was not statistically significant ($\chi^2 = 1.4$, $p = 0.240$). We did not observe a difference between genders for participants reporting no supportive experiences (6 men and 4 women; $p = 1$ using a Fisher's Exact Test).

Multiple mentions of toxic experiences by both genders.

Bullying, harassment, fear of retaliation, and doxxing were reported by women (N=9, 7.9%) and men (N=14, 8.6%; $\chi^2 = 27$, $p = 0.600$). One man shared he experienced "years of harassment, doxxing, and impersonation," including "fake profiles created in white nationalism and hacking forums." Unwanted attention or sexual advances were mentioned by three women and one man. One participant shared, "A somewhat close friend I had made through a cybersecurity forum had made quite a few uncomfortable sexual remarks which made me question if cybersecurity as a whole was like this or if it was an isolated case."

Men and women reported some common experiences. In addition to the differences discussed above, we also observed some similarities in unsupportive experiences, though these were typically less frequent. These included feeling unwelcome as newcomers (18 men, 11.0%; 6 women, 5.3%; $\chi^2 = 1.3715$, p= 0.242), receiving negative consequences from their own actions (13 men, 8.0%; 10 women, 8.8%; $\chi^2 = 0$, $p = 1$), and difficulty collaborating (22 men, 13.5%; 11 women, 9.6%; $\chi^2 = 0.5$, $p = 0.473$).

There was also general agreement on supportive experiences. Men and women both described receiving career support (41 men, 23.8%; 30 women, 26.1%; $\chi^2 = 0.1$, $p = 0.781$), having their questions answered (26 men, 15.1%; 20 women, 17.4%; $\chi^2 = 0.1$, $p = 0.734$), having positive educational experiences (16 men, 9.3%; 7 women, 6.1%; $\chi^2 = 0.6$, $p = 0.444$), and participating in collaborative problem solving (21 men, 12.2%; 11 women, 9.6%; $\chi^2 = 0.3$, $p = 0.608$).

Women receive support from individuals; men more likely to find groups helpful. Women predominantly cited experiences with specific individuals such as managers, professors, and specific friends or acquaintances (N=47). While the same number of men discussed these individual relationships (N=47), this number is proportionally lower (27.3% of men and 40.9% of women) On the other hand, men discussed supportive experiences with broader groups like online forums or conferences more frequently than women did (34 men, 19.8%; 13 women, 11.3%). One man said, "After sharing a blog post or link to code, someone from the community replied with helpful advice or other areas I could investigate."This difference was statistically significant ($\chi^2 = 6.4$, $p = 0.011$). While we saw a similar divide between men and women in terms of the people involved in unsupportive experiences, i.e., individuals (27 men, 16.6%; 26 women, 22.8%) and groups (27 men, 16.6%; 14 women, 12.3%), this difference was not statistically significant ($\chi^2 = 2.1$, $p = 0.147$).

8 Discussion and Recommendations

Our results provide insights into demographic discrepancies in perceived belonging and community experiences among cybersecurity professionals, alongside overarching trends within the community. We distill common themes from our results and propose actionable recommendations for community and organizational leaders to improve inclusivity and diversity.

8.1 Perceived Belonging and Community Experience Themes

There is a clear gender disparity in community experiences. Across all research questions, the primary divide observed was between genders. Women are more likely to face harassment and unwelcoming experiences related to their identity. Likely due to these unwelcoming experiences, women were less likely to participate in general-interest security organizations, instead opting for identity-based groups, similar to anecdotes presented by Fulton et al. [38].

While we did not have a large enough sample of genderqueer participants to produce generalizable results, these participants' responses suggest they face an unwelcoming community. Across all our survey questions, genderqueer participants reported lower perceptions of belonging and higher experiences of unsupportive environments and identity-based harassment. Future work should focus on this group to better understand the unique challenges they face.

While these experiences mirrored examples described by interview participants in prior work [38], our work demonstrates a clear gender gap and indicates the scale of the problem.

Black participants' responses suggest positive outcomes. Turning to differences between races/ethnicities, we only observed significant differences between Black and White participants. Black participants found community organizations more helpful to their development and career success and had higher vulnerability discovery self-efficacy. This is a positive indicator; however, we remain cautious on this finding as the number of Black participants in our sample was small (N=38) and our findings are only indicative of current cybersecurity professionals' experiences, meaning survivor bias likely plays a role in this result. Further, we stress that while we considered differences in high-level demographic groups, the experiences of members of these groups are not monolithic. Further work is needed to confirm these results with a larger sample and assess the impact of intersectional identities.

Safety perceived as low across participants. Across all demographic groups, we observed low psychological safety scores when compared to results of prior surveys [40]. This lack of perceived safety to engage with others in the community could be internal (e.g., impostor syndrome or perceived lack of knowledge), but our measures of internal belonging and knowledge did not show a similar deficit. This suggests the perceived lack of safety is caused by external forces. which is supported by participants' multiple instances of reported harassment experiences across demographic groups. These results suggest efforts to improve inclusivity and climate in the cybersecurity community would be universally beneficial.

This finding also points to a larger issue of survivor bias in our results. Prior work has shown people with low belonging uncertainty [122] and high self-efficacy [61] are better equipped to overcome negative external forces (like those we observed) because they have a strong internal view of self. Conversely, individuals without the same strong internal perception of self may not join, or remain in, the cybersecurity community due to these negative forces. While our results cannot make claims regarding the people excluded from the community, they point to a potentially high dropout rate and motivate future work investigating this problem.

More work is needed to ensure early cybersecurity education is inclusive and supportive. There have been significant efforts to increase early development programs for cybersecurity-interested students [11, 52, 66, 71, 77, 79, 82]. These programs are important, but our results suggest more work is necessary to investigate and improve their associated communities' inclusivity. Our results indicate cybersecurity professionals who begin skill development early are more likely to face unsupportive environments.

We expected early engagement would lead to stronger perceptions of belonging. While higher vulnerability discovery self-efficacy correlated with high-school programming experience, these early experiences also correlated with lower psychological safety and increased reports of severe harassment, particularly among marginalized groups. This likely contributes to higher dropout rates, emphasizing the need for welcoming and inclusive early education.

While we did not find direct evidence about this, we speculate women are more comfortable participating in gender-specific affinity groups than in general support groups, which may relate to the higher rate of severe harassment women reported, as supported by [38], which described participants avoiding certain groups due to negative experiences.

8.2 Community Leaders Recommendations

Our results indicate a need to improve the culture in cybersecurity to make it more safe and inclusive for everyone, especially women/gender minorities and early career cybersecurity professionals. To this end, we draw on existing best practices from prior work in psychological safety evaluated in other domains [31]. For each best practice, we discuss potential adoption strategies, noting that while these practices were designed for structured workplaces, not all cybersecurity organizations fit this mold (e.g., conference communities, online forums). However, we discuss how the ideas of these practices can be leveraged in less structured environments.

Set the stage. The first step to establish a safer, more inclusive community is for leaders to emphasize safety and inclusivity's value and clearly frame participation in cybersecurity as open to all. This step's goal is to set a shared expectation and vision. For example, #ShareTheMicInCyber promotes the stories and accomplishments of Black cybersecurity professionals, highlighting the impact of their work on the field [99]. Additionally, all major security conferences have established codes of conduct [25, 49, 58, 80, 107, 114] and many have adopted diversity and inclusion statements [23, 50, 53, 115] extolling the importance of a welcoming community, indicating goals for inclusivity, and establishes that hate and harassment that will not be tolerated. While there has been a significant increase in this stage setting recently, it is important that these messages are repeated regularly and within all subcommunities.

Invite participation. While setting the stage is important for creating a shared vision in the community, it is not as meaningful if action is not taken to foster inclusivity. Action is not only the responsibility of leaders, but all members because parts of the cybersecurity community lack clear leaders and structure. Unfortunately, the low psychological safety observed suggests cybersecurity professionals may be less likely to stand up as allies. To counter this issue, community leaders should provide training and support that encourage being an ally and bystander intervention [4], more empathetic responses, and a transition away from a victim-blaming.

Responding productively. Finally, it is paramount that cybersecurity professionals experience actual safety when participating in the community through demonstrated support. The most important practice here is to sanction clear instances of hate and harassment, especially targeting women and genderqueer cybersecurity professionals, as those were seen as most prevalent is our results. This response requires transparent and clear guidelines to avoid silencing expression. Our results indicate cybersecurity professionals experience hate and harassment that crosses a clear boundary, according to most existing policies [23, 25, 49, 50, 53, 58, 80, 107, 114, 115], so it is important these actions are sanctioned publicly to demonstrate the community's commitment to inclusivity. In some subcommunities with less structure, sanctions may be harder to employ, as there is limited central control. These cases demonstrate, again, the need to develop a broad culture of inclusion among community members. For example, it may not be possible for moderators to effectively ban offending users on an anonymous site, as these users can just create new accounts. Allies, instead, might respond with support for the victim and make it clear the offenders' views are not acceptable or representative of the subcommunity.

Our results also suggest destigmatizing mistakes for beginners, especially in early development phases. Beginners may ask easily searchable questions, which can seem frustrating for overworked security educators, but should not be met with disdain [118]. Instead, using resources like FAQs and detailed walkthroughs can help. Questions that persist should be addressed with care, as having someone reliable to ask is crucial for development. Practicing empathy and patience is vital, as most cybersecurity professionals experience some insecurity.

9 Acknowledgements

Many thanks to the anonymous reviewers who provided helpful comments on drafts of this paper, WISP [125], #ShareTheMicInCyber [99], and Jordan Wiens for help with recruitment, and Rachel Tobac for valuable insights with the study design. This project was supported by NSF grants CNS-1943215, CNS-1801545, and CNS-2247959 and gifts from Google. The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. MITRE has approved this work for public release and unlimited distribution; public release case number 24-0521.

References

[1] M K Ahuja. Women in the information technology profession: a literature review, synthesis and research agenda. *European Journal of Information Systems*, 11(1):20–34, 2002.

[2] Omer Akgul, Taha Eghtesad, Amit Elazari, Omprakash Gnawali, Jens Grossklags, Michelle L. Mazurek, Aron Laszka, and Daniel Votipka. Bug hunters' perspectives on the challenges and benefits of the bug bounty ecosystem. In *32nd USENIX Security Symposium*, USENIX Sec '23, Los Angeles, CA, August 2022. USENIX Association.

[3] Catherine Ashcraft, Elizabeth Eger, and Michelle Friend. Girls in it: The facts. Technical report, National Center for Women & Information Technology, 2012.

[4] American Psychological Association. Bystander intervention tip sheet. https://www.apa.org/pi/health-equity/bystander-intervention. (Accessed 02-13-2024).

[5] Markus Baer and Michael Frese. Innovation is not enough: climates for initiative and psychological safety, process innovations, and firm performance. *Journal of Organizational Behavior*, 24(1):45–68, 2003.

[6] Shaowen Bardzell and Jeffrey Bardzell. Towards a feminist hci methodology: social science, feminism, and hci. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 675–684, 2011.

[7] Joseph Biden. Executive order on improving the nation's cybersecurity, May 2021. (Accessed 07-21-2021).

[8] Boeing. Boeing technical apprenticeship. https://jobs.boeing.com/btap. (Accessed 01-05-2024).

[9] Amiangshu Bosu and Kazi Zakia Sultana. Diversity and inclusion in open source software (oss) projects: Where do we stand? In *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pages 1–11, 2019.

[10] BugCrowd. Inside the mind of a hacker 2020, 2020. (Accessed 07-21-2020).

[11] Tanner J. Burns, Samuel C. Rios, Thomas K. Jordan, Qijun Gu, and Trevor Underwood. Analysis and exercises for engaging beginners in online CTF competitions for security education. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, August 2017. USENIX Association.

[12] A Colin Cameron and Pravin K Trivedi. *Regression analysis of count data*, volume 53. Cambridge university press, 2013.

[13] Sang-Mi Chai and Min-Kyun Kim. A road to retain cybersecurity professionals: An examination of career decisions among cybersecurity scholars. *Journal of the Korea Institute of Information Security & Cryptology*, 22(2):295–316, 2012.

[14] Nina Chamlou. Diversity in cybersecurity. https://www.cyberdegrees.org/resources/diversity-in-cybersecurity/, 2022.

[15] Sapna Cheryan, Benjamin J. Drury, and Marissa Vichayapai. Enduring influence of stereotypical computer science role models on women's academic aspirations. *Psychology of Women Quarterly*, 37(1):72–79, 2013.

[16] Sapna Cheryan, Allison Master, and Andrew N Meltzoff. Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes. *Frontiers in psychology*, 6:49, 2015.

[17] Sapna Cheryan, Victoria C Plaut, Paul G Davies, and Claude M Steele. Ambient belonging: how stereotypical cues impact gender participation in computer science. *Journal of personality and social psychology*, 97(6):1045, 2009.

[18] Sapna Cheryan, John Oliver Siy, Marissa Vichayapai, Benjamin J Drury, and Saenam Kim. Do female and male role models who embody stem stereotypes hinder women's anticipated success in stem? *Social Psychological and Personality Science*, 2(6):656–664, 2011.

[19] Debbie Clayton and Teresa Lynch. Ten years of strategies to increase participation of women in computing programs: The central queensland university experience: 1999–2001. *SIGCSE Bull.*, 34(2):89–93, jun 2002.

[20] David A Cole, Elizabeth A Nick, Rachel L Zelkowitz, Kathryn M Roeder, and Tawny Spinelli. Online social support for young people: does it recapitulate in-person social support; can it help? *Computers in human behavior*, 68:456–464, 2017.

[21] Christopher J Collins and Ken G Smith. Knowledge exchange and combination: The role of human resource practices in the performance of high-technology firms. *Academy of management journal*, 49(3):544–560, 2006.

[22] Joel Cooper. The digital divide: The special case of gender. *Journal of computer assisted learning*, 22(5):320–334, 2006.

[23] Cas Cremers and Engin Kirda. Diversity and inclusion. https://www.sigsac.org/ccs/CCS2024/code-of-conduct/diversity-and-inclusion.html. (Accessed 02-02-2024).

[24] Robert Gordon Kent de Grey. *Friends in High-Tech Places: The Development and Validation of the Online Social Support Measure*. PhD thesis, The University of Utah, 2018.

[25] Code of conduct. https://defcon.org/html/links/dc-code-of-conduct.html. (Accessed 02-13-2024).

[26] Anne Deiglmayr, Elsbeth Stern, and Renate Schubert. Beliefs in "brilliance" and belonging uncertainty in male and female stem students. *Frontiers in psychology*, 10:442252, 2019.

[27] James R Detert and Ethan R Burris. Leadership behavior and employee voice: Is the door really open? *Academy of management journal*, 50(4):869–884, 2007.

[28] Michelle Drolet. Diversity in cybersecurity: Barriers and opportunities for women and minorities. https://www.csoonline.com/article/571811/diversity-in-cybersecurity-barriers-and-\opportunities-for-women-and-minorities.html, 2021.

[29] Michael H. Dunn and Laurence D. Merkle. Assessing the impact of a national cybersecurity competition on students' career interests. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, SIGCSE '18, page 62–67, New York, NY, USA, 2018. Association for Computing Machinery.

[30] Amy Edmondson. Psychological safety and learning behavior in work teams. *Administrative science quarterly*, 44(2):350–383, 1999.

[31] Amy C Edmondson. *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. John Wiley & Sons, 2018.

[32] Rachel Fairbank. Psychologists persevere in edi work despite growing backlash against racial equity efforts. https://www.apa.org/monitor/2024/01/trends-anti-equity-diversity-inclusion-laws, 2024. (Accessed 02-08-2024).

[33] Ronald A Fisher. On the interpretation of χ 2 from contingency tables, and the calculation of p. *Journal of the Royal Statistical Society*, 85(1):87–94, 1922.

[34] Cynthia E Foor, Susan E Walden, and Deborah A Trytten. "i wish that i belonged more in this whole engineering group:" achieving individual diversity. *Journal of Engineering Education*, 96(2):103–115, 2007.

[35] National Initiative for Cybersecurity Careers and Studies. Cybersecurity education and training assistant program. https://niccs.cisa.gov/cybersecurity-career-resources/cybersecurity-education-and-training-assistance-program. (Accessed 01-05-2024).

[36] National Initiative for Cybersecurity Education. National initiative for cybersecurity education cybersecurity workforce framework. https://www.cisa.gov/national-initiative-cybersecurity-education-\nice-cybersecurity-workforce-framework. (Accessed 01-05-2024).

[37] Karl Pearson F.R.S. X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine*, 50(302):157–175, 1900.

[38] Kelsey R. Fulton, Samantha Katcher, Kevin Song, Marshini Chetty, Michelle L. Mazurek, Chloé Messdaghi, and Daniel Votipka. Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery. In *Proceedings of the 44th IEEE Symposium on Security and Privacy*, IEEE S&P '23, 2023.

[39] Kelsey R. Fulton, Daniel Votipka, Desiree Abrokwa, Michelle L. Mazurek, Michael Hicks, and James Parker. Understanding the how and the why: Exploring secure development practices through a course competition. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, New York, NY, USA, 2022. Association for Computing Machinery.

[40] David A Garvin, Amy C Edmondson, and Francesca Gino. Is yours a learning organization? *Harvard business review*, 86(3):109, 2008.

[41] Thomas Gilovich, Dacher Keltner, and Richard E Nisbett. Being a member of a stigmatized group: stereotype threat. *Gilovich, Thomas; Keltner, Dacher; Nisbett, Richard E., Social psychology, New York: WW Norton*, pages 467–468, 2006.

[42] John W. Graham and Steven A. Smith. Gender differences in employment and earnings in science and engineering in the us. *Economics of Education Review*, 24(3):341–354, 2005.

[43] Robert G Kent de Grey, Bert N. Uchino, Brian RW Baucom, Timothy W. Smith, Avery E. Holton, and Edward F. Diener. Enemies and friends in high-tech places: the development and validation of the online social experiences measure. *Digital Health*, 5(1), 2019.

[44] HackerOne. 2019 hacker-powered security report. Technical report, HackerOne, San Francisco, California, December 2019.

[45] HackerOne. The 2020 hacker report. Technical report, HackerOne, San Francisco, California, December 2020.

[46] Andrew F Hayes and Klaus Krippendorff. Answering the call for a standard reliability measure for coding data. *Communication methods and measures*, 1(1):77–89, 2007.

[47] Eoin Hinchy. Voice of the soc analyst. https://www.tines.com/reports/voice-of-the-soc-analyst, 2022.

[48] Andrew Gary Darwin Holmes. Researcher positionality–a consideration of its influence and place in qualitative research–a new researcher guide. *Shanlax International Journal of Education*, 8(4):1–10, 2020.

[49] Code of conduct. https://www.blackhat.com/code-of-conduct.html. (Accessed 02-13-2024).

[50] Diversity and inclusion. https://www.blackhat.com/html/sustainability.html. (Accessed 02-13-2024).

[51] Ohio Cyber Range Insitute. Ohio cyber range institute: Unlocking potential, securing the future. https://www.ohiocyberrangeinstitute.org/. (Accessed 01-06-2024).

[52] SANS Cybersecurity Institute. Girls go cyberstart. (Accessed 05-27-2020).

[53] Diversity and inclusion. https://www.ieee.org/about/diversity-index.html. (Accessed 02-13-2024).

[54] ISC2. Isc2 cybersecurity workforce study 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e, 2023.

[55] Shanto Iyengar, Gaurav Sood, and Yphtach Lelkes. Affect, Not Ideology: A Social Identity Perspective on Polarization. *Public Opinion Quarterly*, 76(3):405–431, 09 2012.

[56] Harjot Kaur, Sabrina Amft, Daniel Votipka, Yasemin Acar, and Sascha Fahl. Where to recruit for security development studies: Comparing six software developer samples. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 4041–4058, 2022.

[57] Robert G Kent de Grey, Bert N Uchino, Brian RW Baucom, Timothy W Smith, Avery E Holton, and Edward F Diener. Enemies and friends in high-tech places: the development and validation of the online social experiences measure. *Digital Health*, 5:2055207619878351, 2019.

[58] Engin Kirda and David Lie. Code of conduct. https://www.sigsac.org/ccs/CCS2024/code-of-conduct/code-of-conduct.html. (Accessed 02-02-2024).

[59] Solomon Klappholz. A third of cyber security pros report crumbling work-life balance. https://www.itpro.com/security/a-third-of-cyber-security-pros-report-crumbling-\work-life-balance, 2023.

[60] Andrew J Ko. Attitudes and self-efficacy in young adults' computing autobiographies. In *2009 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 67–74. IEEE, 2009.

[61] Robert W. Lent, Steven D. Brown, and Gail Hackett. Toward a unifying social cognitive theory of career and academic interest, choice, and performance. *Journal of Vocational Behavior*, 45(1):79 – 122, 1994.

[62] Jian Liang, Crystal I. C. Farh, and Jiing-Lih Farh. Psychological antecedents of promotive and prohibitive voice: A two-wave examination. *Academy of Management Journal*, 55(1):71–92, 2012.

[63] Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. Given enough eyeballs, all bugs are shallow? revisiting eric raymond with bug bounty programs. In *Proceedings of the 15th Workshop on the Economics of Information Security*, WEIS '16, 2016.

[64] Jane Margolis, Rachel Estrella, Joanna Goode, Jennifer Jellison Holme, and Kim Nao. *Stuck in the shallow end: Education, race, and computing*. MIT press, 2017.

[65] Jane Margolis and Allan Fisher. *Unlocking the clubhouse: Women in computing*. MIT press, Cambridge, MA, 2002.

[66] Luke McCormack. Us cyber challenge. https://www.uscyberchallenge.org/, September 2022. (Accessed 09-17-2022).

[67] Robert K McKinley, Terjinder Manku-Scott, Adrian M Hastings, David P French, and Richard Baker. Reliability and validity of a new measure of patient satisfaction with out of hours primary medical care in the united kingdom: development of a patient questionnaire. *Bmj*, 314(7075):193, 1997.

[68] Adam W Meade and S Bartholomew Craig. Identifying careless responses in survey data. *Psychological methods*, 17(3):437, 2012.

[69] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M Angela Sasse, and Imogen Verret. Why it security needs therapy. In *European Symposium on Research in Computer Security*, pages 335–356. Springer, 2021.

[70] Rachel Minkin. Personal experiences with online harassment. https://www.pewresearch.org/social-trends/2023/05/17/diversity-equity-and-inclusion-in-the-workplace/, 2023. (Accessed 02-08-2024).

[71] Jelena Mirkovic and Peter A. H. Peterson. Class capture-the-flag exercises. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, San Diego, CA, August 2014. USENIX Association.

[72] Phoenix Moorman and Elizabeth Johnson. Still a stranger here: Attitudes among secondary school students towards computer science. In *Proceedings of the 8th Annual Conference on Innovation and Technology in Computer Science Education*, ITiCSE '03, page 193–197, New York, NY, USA, 2003. Association for Computing Machinery.

[73] Laurie A. Morgan. Glass-ceiling effect or cohort effect? a longitudinal study of the gender earnings gap for engineers, 1982 to 1989. *American Sociological Review*, 63(4):479–493, 1998.

[74] Dawn Nafus. 'patches don't have gender': What is not open in open source software. *New Media & Society*, 14(4):669–683, 2012.

[75] Elizabeth A Nick, David A Cole, Sun-Joo Cho, Darcy K Smith, T Grace Carter, and Rachel L Zelkowitz. The online social support scale: measure development and validation. *Psychological assessment*, 30(9):1127, 2018.

[76] SH Nielsen, LA von Hellens, and Sharon Wong. The male it domain: You've got to be in it to win it. In *Proceedings of the 12th Australasian Conference on Information Systems (ACIS 2001)*, pages 1–12, 2001.

[77] NIST. Cybersecurity competitions | nist. https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council/cybersecurity-skills-0, 2023. (Accessed 02-08-2024).

[78] Samantha Nix and Lara Perez-Felkner. Difficulty orientations, gender, and race/ethnicity: An intersectional analysis of pathways to stem degrees. *Social Sciences*, 8(2), 2019.

[79] Plaid Parliament of Pwning. picoctf. https://picoctf.com/. (Accessed 05-27-2020).

[80] IEEE Symposium on Security and Privacy. Code of conduct. https://www.ndss-symposium.org/ndss-code-of-conduct/. (Accessed 02-13-2024).

[81] Zhen Xin Ong, Liz Dowthwaite, Elvira Perez Vallejos, Mat Rawsthorne, and Yunfei Long. Measuring online wellbeing: a scoping review of subjective wellbeing measures. *Frontiers in psychology*, 12:616637, 2021.

[82] PACTF. Pactf. https://2019.pactf.com/. (Accessed 05-27-2020).

[83] Toni C Plato. Women c-suite executives in cybersecurity: Transformational experiences and gender barriers on their leadership journeys, 2021.

[84] Portia Pusey, Mark Gondree, and Zachary Peterson. The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, 14(6):90–95, 2016.

[85] Laura Quintana. Hack your way to a new career in cybersecurity: Cisco networking academy offers new ethical hacker course. https://blogs.cisco.com/learning/hack-your-way-to-a-new-career-in-cybersecurity, October 2023. (Accessed 01-05-2024).

[86] Jessica Rafaeil. How three stem leaders forged a path for others through fearlessness. *US Black Engineer and Information Technology*, 44(1):22–25, 2020.

[87] Adrian E Raftery. Bayesian model selection in social research. *Sociological methodology*, pages 111–163, 1995.

[88] Laurie A Rudman. Self-promotion as a risk factor for women: the costs and benefits of counterstereotypical impression management. *Journal of personality and social psychology*, 74(3):629, 1998.

[89] David L Sackett. Bias in analytic research. In *The case-control study consensus and controversy*, pages 51–63. Elsevier, 1979.

[90] Robert J Sampson. Local friendship ties and community attachment in mass society: A multilevel systemic model. *American sociological review*, pages 766–779, 1988.

[91] Koen Schoenmakers, Daniel Greene, Sarah Stutterheim, Herbert Lin, and Megan J Palmer. The security mindset: characteristics, development, and consequences. *Journal of Cybersecurity*, 9(1):tyad010, 2023.

[92] Elaine Seymour and Nancy M. Hewitt. *Talking About Leaving: Why Undergraduates Leave the Sciences*. Westview Press, 2000.

[93] Jenessa R. Shapiro and Amy M. Williams. The role of stereotype threats in undermining girls' and women's performance and interest in stem fields. *Journal on Sex Roles*, 66(3):175–183, 2012.

[94] Enno Siemsen, Aleda V Roth, Sridhar Balasubramanian, and Gopesh Anand. The influence of psychological safety and confidence in knowledge on employee knowledge sharing. *Manufacturing & service operations management*, 11(3):429–447, 2009.

[95] Daryl G Smith. *Diversity's Promise for Higher Education: Making It Work*. JHU Press, 2020.

[96] Elliott Sober. Instrumentalism, parsimony, and the akaike framework. *Philosophy of Science*, 69(S3):S112–S123, 2002.

[97] David M. Sparks, Steve Daniel Przymus, Allison Silveus, Yohanis De La Fuente, and Cassandra Cartmill. Navigating the intersectionality of race/ethnicity, culture, and gender identity as an aspiring latina stem student. *Journal of Latinos and Education*, 22(4):1355–1371, 2023.

[98] Claude M. Steele, Steven J. Spencer, and Joshua Aronson. Contending with group image: The psychology of stereotype and social identity threat. volume 34 of *Advances in Experimental Social Psychology*, pages 379–440. Academic Press, 2002.

[99] Camille Stewart, Lauren Zabierek, and Katelyn Ringrose. #sharethemicincyber. https://www.sharethemicincyber.com/.

[100] Anselm Strauss and Juliet Corbin. *Basics of qualitative research*, volume 15. Newbury Park, CA: Sage, 1990.

[101] Supplemental materials. https://osf.io/k3m8g.

[102] Synack. Synack cybersecurity diversity and inclusion report. https://www.synack.com/diversity-report/, 2020.

[103] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2023.

[104] Mohammad Tahaei and Kami Vaniea. Recruiting participants with programming skills: A comparison of four crowdsourcing platforms and a cs student mailing list. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.

[105] Josh Terrell, Andrew Kofink, Justin Middleton, Clarissa Rainear, Emerson Murphy-Hill, Chris Parnin, and Jon Stallings. Gender differences and bias in open source: Pull request acceptance of women versus men. *PeerJ Computer Science*, 3:e111, 2017.

[106] Steven Terrell and Kembley Lingelbach. A study of female cybersecurity professionals. *Issues in Information Systems*, 24(3), 2023.

[107] Code of conduct. https://www.ndss-symposium.org/ndss-code-of-conduct/. (Accessed 02-13-2024).

[108] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 247–267, 2021.

[109] Eileen M Trauth. Mapping information-sector work to the work force. *Communications of the ACM*, 44(7):74–75, 2001.

[110] Thomas Trevethan and Grace Williams. The time is now to secure the future. https://www.paloaltonetworks.com/blog/2023/10/secure-the-future/, October 2023. (Accessed 01-06-2024).

[111] Chih-Hsiung Tu. The measurement of social presence in an online learning environment. In *International Journal on E-learning*, volume 1, pages 34–45. Association for the Advancement of Computing in Education (AACE), 2002.

[112] Sherry Turkle. *The Second Self: Computers and the Human Spirit*. Mit Press, 1984.

[113] Visa University. Visa payments cybersecurity certification. https://www.visauniversity.com/en/certificate-programs/visa-certification/visa-payments-cybersecurity-certification. (Accessed 01-06-2024).

[114] Code of conduct. https://www.usenix.org/conferences/coc. (Accessed 02-13-2024).

[115] Diversity and inclusion. https://www.usenix.org/conferences/diversity-and-inclusion. (Accessed 02-13-2024).

[116] Bogdan Vasilescu, Daryl Posnett, Baishakhi Ray, Mark G.J. van den Brand, Alexander Serebrenik, Premkumar Devanbu, and Vladimir Filkov. Gender and tenure diversity in github teams. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 3789–3798, New York, NY, USA, 2015. Association for Computing Machinery.

[117] Emily A. Vogels. Personal experiences with online harassment. https://www.pewresearch.org/internet/2021/01/13/personal-experiences-with-online-harassment/, 2021. (Accessed 01-06-2024).

[118] D. Votipka, E. Zhang, and M. Mazurek. Hacked: A pedagogical analysis of online vulnerability discovery exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1589–1606, Los Alamitos, CA, USA, may 2021. IEEE Computer Society.

[119] Daniel Votipka, Desiree Abrokwa, and Michelle L. Mazurek. Building and validating a scale for secure software development self-efficacy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–20, New York, NY, USA, 2020. Association for Computing Machinery.

[120] Daniel Votipka, Hongyi Hu, Bryan Eastes, and Michelle L. Mazurek. Toward a field study on the impact of hacking competitions on secure development. In *Proceedings of the 4th Workshop on Security Information Workers*, WSIW '18, Baltimore, MD, 2018. USENIX Association.

[121] Daniel Votipka, Rock Stevens, Elissa M Redmiles, Jeremy Hu, and Michelle L Mazurek. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *Proceedings of the 39th IEEE Symposium on Security and Privacy*, IEEE S&P '18, 2018.

[122] Gregory M Walton and Geoffrey L Cohen. A question of belonging: race, social fit, and achievement. *Journal of personality and social psychology*, 92(1):82, 2007.

[123] Miranda Wei, Pardis Emami-Naeini, Franziska Roesner, and Tadayoshi Kohno. Skilled or gullible? gender stereotypes related to computer security and privacy. In *IEEE Symposium on Security and Privacy*, 2023.

[124] Elizabeth Williams. Actualizing gender and racial diversity inclusion in computing fields. *Issues in Information Systems*, 24(4), 2023.

[125] Women in security and privacy. https://www.wisporg.com/, 2024.

[126] Danielle M. Young, Laurie A. Rudman, Helen M. Buettner, and Meghan C. McLean. The influence of female role models on women's implicit science cognitions. *Psychology of Women Quarterly*, 37(3):283–292, 2013.

A Survey

Helpfulness Scale. Extremely helpful, Somewhat helpful, Neither helpful nor unhelpful, Somewhat unhelpful, Extremely unhelpful

Agreement Scale. Strongly disagree, Disagree, Somewhat disagree, Neither agree nor disagree, Somewhat agree, Agree, Strongly agree

A.1 General Belonging

This section asks about your experiences in the cybersecurity community and any support in these settings you have been provided toward your security education and career.

For the following statements, please indicate the extent to which they reflect your experience in the cybersecurity community. *1 (Very inaccurate), 2, 3, 4 (Neither accurate nor inaccurate), 5, 6, 7 (Very accurate)*

1. In cybersecurity spaces, it is easy to speak up about what is on your mind.
2. If you make a mistake in the cybersecurity community, it is often held against you.
3. People in cybersecurity are usually comfortable talking about problems and disagreements.
4. People in cybersecurity are eager to share information about what doesn't work as well as share information about what does work.
5. Keeping your cards close to your chest is the best way to get ahead in the cybersecurity community.

Please indicate your level of agreement with the following statements: *Agreement Scale*

1. Sometimes I feel that I belong in cybersecurity, and sometimes I feel that I don't belong.
2. When something bad happens, I feel that maybe I don't belong in cybersecurity.
3. When something good happens, I feel that I really belong in cybersecurity.
4. People from different backgrounds have equal opportunities to participate in the cybersecurity community.

For the following items, think about your interactions with your professors/peers/collegues in the computer security community. To respond, indicate to what extent you felt this way. *Very Slightly or Not at all, A Little, Moderately, Quite a Bit, Extremely*

1. Interactions with someone in the field prevented me from working on my goals or other important things.
2. Someone in the cybersecurity community has encouraged me when I felt like quitting.
3. I have felt supported by someone in the cybersecurity community who agreed with my point of view.
4. I have been unable to fall asleep while thinking about a negative interaction I had with someone in the cybersecurity community.
5. There are people in the cybersecurity community please ignore the first part of this statement and mark "Extremely".
6. Someone in the cybersecurity community has cheered me up when I was feeling down.
7. Someone in the cybersecurity community has made me feel embarrassed or foolish.
8. There is someone in the cybersecurity community I can turn to for advice about handling problems.
9. There is someone in the cybersecurity community I could turn to for advice about making career plans or about changing my job.

Have you ever experienced any of the following behaviors directed at you in the context of the cybersecurity community? *Never, Rarely, Occasionally, Frequently*

1. Lack of response or rejection of contributions or questions.
2. Conflict or interpersonal tension between you and another community member.
3. Written or spoken language that made you feel unwelcome (e.g. profanity, racist jokes, sexual imagery, hostility, rudeness, name calling).
4. Stereotyping based on perceived demographic characteristics.
5. Threats of violence, stalking.
6. Unsolicited sexual advance or comments.
7. Impersonation or malicious publication of personal information (doxxing).

A.2 Close Relations

This section asks about your experience with family, friends and other close mentors, and any support they have provided toward your security education and career.

1. Do you have an family, friends or other close mentors you go to for help when you're trying to learn difficult security concepts? *Yes, one; Yes, a few; Yes, many; No*
2. How often do you discuss technical topics related to your security education and career with your family/friends/-mentors? *Never, Rarely, Occasionally, Frequently*
3. How helpful do you find the security-related guidance that your family/friends/mentors give you? *Helpfulness scale*

A.3 Workplace

This section asks about your experiences in your workplace and any support in these settings you have been provided toward your security education and career.

1. Are you a part of any workplaces where security concepts are discussed? *Yes, but security concepts are rarely discussed; Yes, security concepts are sometimes discussed; Yes, security concepts are often discussed; No, but I was previously employed in security; No*
2. What is the primary focus of the company you work for? *Non-technical - critical infrastructure (hospitals, power, etc.), Non-technical - non-critical infrastructure, Security - defense (intrusion detection/response, system defense/hardening), Security - offense (penetration testing, vulnerability analysis), Other technical - software development, Other technical - network/system administration, Other technical - hardware development, Other*
3. How often do you discuss technical topics related to your security education and career in your workplace? *Never, Rarely, Occasionally, Frequently*
4. How helpful do you find the security-related guidance given to you by colleagues in your workplace? *Helpfulness scale*

A.4 Organizations

This section asks about your experience with any organizations you participate in and any support you have received toward your security education or career. We consider an organization as any group outside your work/-classes where people meet regularly to discuss technical topics of interest (e.g., local ACM chapter, Women in Security and Privacy). Please answer the following questions only considering security-related organizations.

1. Are you a part of any organizations where security concepts are discussed? *Yes, I participate in one organization where security concepts are discussed; Yes, I participate in a few organizations where security concepts are discussed; Yes, I participate in many organizations where security concepts are discussed; No*
2. What kinds of organizations are you a part of? *"Identity-based (e.g. Women in Security, LGBTQ+ in Security, Blacks in Cyber)", "Topic-based (e.g. malware analysis working group)", "General security group", "Other"*
3. How often do you discuss technical topics related to your security education and career with people in these organizations? *Never, Rarely, Occasionally, Frequently*
4. How helpful do you find the security-related guidance given to you by people in organizations you are a part of? *Helpfulness scale*

A.5 School

This section asks about your experiences in your school and any support in these settings you have been provided toward your security education and career. This section only pertains to academic situations, e.g., classes, professors, peers, organizations.

1. Have you taken any classes where security concepts are discussed? *Yes, one; Yes, a few; Yes, many; No*
2. Are you a part of any school organizations where security concepts are discussed? *Yes, I participate in one organization where security concepts are discussed; Yes, I participate in a few organization where security concepts are discussed; Yes, I participate in many organization where security concepts are discussed; No*
3. How often do you discuss technical topics related to your security education in your school? *Never, Rarely, Occasionally, Frequently*
4. How helpful do you find the security-related guidance given to you by professors and peers? *Helpfulness scale*

A.6 Broader Security Community

This section asks about your experience with the broader security community, including conferences/workshops or online when asking questions about or discussing computer security topics. We define online community discussions as any discussion about security concepts in a public online forum (e.g., StackOverflow, Reddit, Twitter, public Slack or Discord).

1. Have you participated in the broader security community (conferences/workshops or online security communities)?

   'Yes, I participate in one public conference or online community; Yes, I participate in a few public conferences or online communities; Yes, I participate in many public conferences or online communities; No
2. Please indicate any security conferences or workshops you have participated in.

3. Please indicate any forums or social media platforms you use for interacting with the public online security community.

4. How often do you discuss technical topics related to your security education and career with people in the broader security community? *Never, Rarely, Occasionally, Frequently*

5. How helpful do you find the security-related guidance given to you by people in the broader security community? *Helpfulness scale*

A.7 General

We have asked several questions pertaining to your experiences with various communities surrounding you—close contacts, school/workplaces, organizations, and the broader security community. For the next section, we'll ask you to consider all the experiences you've had with others in the security community. For both questions, we ask that you do not name specific individuals.

1. Please describe one particularly good experience you had with a community you are part of (and mention which community—close contacts, school/workplaces, organizations, or the broader security community). This could be any experience where you felt the other individual was supportive and helped your development or career in a tangible or intangible way.

2. Please describe one particularly bad experience you had with a community you are part of (and mention which community—close contacts, school/workplaces, organizations, or the broader security community). This could be any experience where you felt the other individual was not supportive and the interaction was harmful to your development or career in a tangible or intangible way.

Now we will ask some questions pertaining to your background and experience in computer security.

1. Do you work in a role where you are asked to perform security tasks? *Yes, this is the primary focus of my job; Yes, this is a part of my job, but not the primary focus; I previously worked in a role where security was my primary focus; I previously worked in a role where security was part of the job; No*

2. Please indicate the approximate number of years you have worked in security.

3. What is/was your position title?

4. Did you choose to leave? *Yes, No*

5. If you feel comfortable sharing, what were your reasons for leaving?

Please indicate your level of agreement with the following statements: *Agreement Scale*

1. I am interested in continuing my security education.

2. I am interested in pursuing or continuing to pursue a career in security.

3. I am well-prepared for a career in security.

Please indicate:

1. Have you participated in any of the following types of security education? (Select all that apply) *Capture-the-flag, wargames, or other online security competitions (e.g., picoCTF, crackmes, iCTF), Penetration testing lab (e.g., Hack the box) or cyber range exercise, Professional certification course (e.g., GIAC Security Essentials, Certified Ethical Hacker), Conference workshop (e.g., Defcon Village workshops), MOOC security course (e.g., Coursera Cybersecurity Specialization), Academic course, Other, I have not participated in any security education*

2. Where did you typically rank when participating in CTFs or other online security competitions? *Top 25% of participants, 25-50% of participants, 50-75% of participants, Bottom 25% of participants*

Please indicate how confident you are in the following statements: *Not confident at all, Slightly confident, Somewhat confident, Moderately confident, Absolutely confident*

1. I can perform a threat risk analysis (e.g., likelihood of vulnerability, impact of exploitation)

2. I can identify potential security threats to the system

3. I can identify the common attack techniques used by attackers

4. I can identify potential attack vectors in the environment the system interacts with (e.g., hardware, libraries)

5. I can identify common vulnerabilities of a programming language

6. I can identify the common please ignore this question and select "Absolutely confident"

7. I can design software to quarantine an attacker if a vulnerability is exploited

8. I can mimic potential threats to the system

9. I can evaluate security controls on the system's interfaces/interactions with other software systems

10. I can evaluate security controls on the system's interfaces/interactions with hardware systems

Cybersecurity development experiences

1. When was the earliest time you remember first being interested in computer security? Please indicate your approximate age: *(Number)*
2. When was the earliest time you had someone (e.g., friend, family member, colleague) in your life who you could go to for security education support? Please indicate your approximate age: *(Number)*
3. Aside from direct educational support, do you have anyone (e.g., friend, family member, colleague) who support your educational pursuits in security (e.g., encouragement, monetary support)? *Yes, I have one person who has provided non-educational support; Yes, I have a few people who have provided non-educational support; Yes, I have many people who have provided non-educational support; No*
4. When was the earliest time you had someone (e.g., friend, family member, colleague) in your life who supported your pursuit of a security education aside from direct teaching? Please indicate your approximate age: *(Number)*

A.8 Demographics

1. In which country do you currently reside?
2. How old are you? *18-19, 20-24, 25-29, 30-35, 35-39, 40-44 , 45-49, 50-54, 55+, Prefer not to answer*
3. What is your ethnicity? *White or of European descent, South Asian, Hispanic or Latino/a/x, Middle Eastern , East Asian, Black or of African descent, Southeast Asian, Indigenous (such as Native American, Pacific Islander, or Indigenous Australian), Prefer to self-describe, Prefer not to answer*
4. What is your gender? *Woman, Man, Transgender Woman / Trans Feminine, Transgender Man / Trans Masculine, Non-Binary / Genderqueer / Gender Fluid, Two Spirit, Prefer to state, Prefer not to answer*
5. What is your sexual orientation? Do you identify as: *Bisexual, Gay/Lesbian, Heterosexual/Straight, Don't know, Prefer to self-describe, Prefer not to say*
6. What is the highest degree or level of school you have completed? *High school, Some college or currently enrolled, Associate's degree, Bachelor's degree, Master's/ Professional degree, Doctorate degree, Prefer not to say*
7. Did you take any programming classes or training in high school? *Yes, one; Yes, a few; Yes, many; No*
8. Which range matches most closely your total, pre-tax household income over the last fiscal year? *$< \$29{,}999$, $30,000 - $49,999, $50,000 - $74,999, $75,000 - $99,999, $100,000 - $124,999 , $125,000 - $149,999, $150,000 - $174,999 , $175,000 - $199,999 , $> \$200{,}000$, Prefer not to answer*
9. Which range matches most closely your total, pre-tax household income when growing up? (before 18 years old)? *Same as Question 8*

A.9 Final

1. If you like, we may contact you for one of the following reasons. Please indicate what you like to be contacted for (you may select multiple): *Follow-up interview (i.e., questions related to this study); Future research (i.e., questions related to other computer security topics); Raffle for one of 25 $50 Amazon gift cards; None of the above*
2. Please provide your email address so we can contact you for the reasons selected previously. If you chose to only be contacted for the raffle, your email address will be deleted after the raffle has been completed. Your email will not be used for any purpose beyond those you indicated in the previous question.