Research in human factors increasingly considers disparate harm across identities; I have been a part of this movement, presenting work [1] at "The Center for Privacy and Security for Marginalized and Vulnerable Populations" workshop[1]. To perform such research, the community needs diverse perspectives to ensure that the needs of as many populations as possible are considered; however, investigating barriers and promoting diversity and inclusivity within the research community itself is an essential, yet often unmet task. To help promote diverse voices in our community, I investigate barriers towards inclusivity in computer security publications, promote diverse and underrepresented researchers, and perform community outreach to make the field welcoming to K-12 students.

Addressing Inclusivity in Research. Security is increasingly focused on addressing differential harm across identities; however, inappropriate methods can also inflict harm and disincentivize contributions from marginalized voices. My research investigates barriers and improvements to inclusivity in our community. When investigating demographics and security behaviors, inappropriate analyses can harm identities, e.g., by essentializing groups to insecure practices. In [2], I analyze 138 security papers that use sociodemographics to quantitatively explain security behavior. I find that certain groups are systematically excluded (e.g., non-binary people), methodological issues are prevalent (e.g., confounding variables), and a litany of conflicting results for several demographics. Based on this, I then produced a guide of recommended practices to engage in better methodological practices when analyzing sociodemographics.

When addressing computer-mediated hate, publications may include examples of hateful content and thus need to provide reader protection via content warnings or transformations; however, this is not standardized and often not applied. I have reviewed papers that have contained examples of hate towards religions, races, and genders; I also personally know that reading such content has caused several researchers pain. To address this, I am actively measuring how content protections are applied in security publications. To understand how harmful content can present itself, I will interview researchers in computer security about such experiences. From these insights, I will establish guidelines for the safe presentation of content to minimize reader harm and promote reader diversity.

Promotion of Researcher Diversity. When analyzing human factors, having a diverse set of voices among the research team is not only important for social justice, but a methodological necessity. As the research team is intangibly connected with how the research was conducted, analyzed, and presented, my most recent papers [1,2] contain positionality statements that situate the backgrounds and perspectives the team comes with. Ensuring that these perspectives are diverse and include backgrounds that are often underrepresented is something I prioritize. As a graduate student, I have taken steps to promote diversity within our lab by intentionally working with groups such as *CRA-widening participation*, *DHS-Minority Serving Institution Programs*, and *Illinois CS STARS*. As a result, the four undergraduate researchers I helped mentor are from traditionally underrepresented backgrounds in computing. I am committed to continuing this as a faculty member by building a lab whose strength is derived from the diverse perspectives promoted through it.

K-12th Outreach. While efforts to be more inclusive in our current community are necessary, these efforts must also start earlier; my outreach to K-12 students is part of that. For the past four years, I've developed and taught a "Cybersecurity Ninja Training" course at Illinois CS SAIL to show high schoolers what the field of cybersecurity is. By performing a series of simple exploits against faulty web security, cryptography, software security, and human factors, I show the students how security is fundamentally an adversarial game they can help win. Beyond direct outreach, I also translated [3] into an educational article for K-12 students. Through this, young students can learn in simple terms what state-of-the-art research is, and that working on it is within their grasp. As a faculty member, I will continue making academia accessible to young students of all backgrounds via sustained outreach to the local community, and continued translation of academic works to accessible formats.

[1] The Center for Privacy and Security for Marginalized and Vulnerable Populations. https://prism.eng.ufl.edu, 2023.

References.

[1] **Jaron Mink**, Miranda Wei, Collins W. Munyendo, Kurt Hugenberg, Tadayoshi Kohno, Elissa M. Redmiles, Gang Wang. “It's Trying Too Hard To Look Real: Deepfakes Moderation Mistakes and Identity-Based Bias”. *Under Revision at CHI*, 2024.

[2] Miranda Wei, **Jaron Mink**, Tadayoshi Kohno, Elissa M. Redmiles, Franziska Roesner. “SoK or So(L)K? On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors”. *Under Revision at USENIX Security*, 2024.

[3] **Jaron Mink**, Licheng Luo, Natã M. Barbosa, Olivia Figueira, Yang Wang, and Gang Wang. “DeepPhish: Understanding User Trust Towards Artificially Generated Profiles in Online Social Networks”. In *Proc. of USENIX Security*, 2022.