Jenn Mvongo, Luis Arellano, Yong Kim
W215 Usable Privacy and Security, UC Berkeley MICS
December 12, 2020

Who Do You Trust?

Exploring trust at the intersection of race and cybersecurity advice and help.

Introduction: Motivation and Research Question

With race-related events occurring with more frequency throughout the United States, a reinvigorated focus on rooting out systemic racism from all facets of our society is also occurring. Lisa Ho, Director for UC Berkeley's MICS program recently challenged the student community to consider how systemic racism manifests within cybersecurity. As part of the response and our own personal interest in understanding how race-based topics impact security, we proposed studying the trust people have with different entities providing cybersecurity advice and help. Camille Stewart, former senior policy adviser for cyber, infrastructure and resilience policy at the Department of Homeland Security under President Barack Obama, stated: *"Understanding the cultural nuances of technology use and access is integral to building policies and technical solutions that secure systems and serve people...Racism breeds distrust in systems and institutions."*[1] Usability within cybersecurity and privacy continues to be studied and while the body of knowledge continues to grow, research at the intersection of race and cybersecurity is sparse. However, we have strong evidence that cultural and race factors do play an important part in the overall efficacy of our security systems. For example, Russian GRU agents deliberately targeted specific ethnic communities within the United States with disinformation campaigns to influence the United States 2016 Presidential Elections.[2]

One key reason Russion GRU agents targeted specific ethnic groups and demographics within the United States was because of the evolving trust landscape between the physical and digital realms. People's identities, trust, and technology have become inextricably linked (Marotski, 2003).[3] The increasing prevalence of information

[1] Stewart, Camille. "Systemic Racism Is a Cybersecurity Threat," June 16, 2020. https://www.cfr.org/blog/systemic-racism-cybersecurity-threat.

[2] U.S. Senate, 116th Congress, 1st Session, "Russion Active Measures Campaigns and Interference in the 2016 U.S. Election," August 18, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

[3] Marotzki W., Dittmann J., Lesske F. (2003) Virtual Communities: Trust, Identity, Participation, and Technology. In: Schneider J., Strothotte T., Marotzki W. (eds) Computational Visualistics, Media

technologies in the management of our everyday lives creates an even stronger reliance and increasing levels of trust placed in these technologies. As a source of trusted news, people have looked towards social media sites for information and confirmation. When news or information comes from a trusted person/profile on an online social platform, that piece becomes even more trustworthy. In other words, people are more likely to believe the validity of information from an online identity that seems legitimate, shares personal traits, and is broadcasted on a trusted piece of technology. Discovering this, Russian GRU disinformation campaigns were more successful when targeting specific ethnic and demographic groups.

The research at this critical junction, race and cybersecurity, is still relatively nascent leaving a broad array of questions to pursue.[4] In this paper we look at trust defined by the Oxford Languages Dictionary as a *"firm belief in the reliability, truth, ability, or strength of someone or something."* Trust is a necessary component of our societies and allows us to make the numerous decisions we need to make throughout the day. Without trust in people and technology, it would be impossible to accomplish the amount of work and tasks we need to accomplish throughout the day. Similarly, knowing who to trust for cybersecurity advice and help could mean the difference between compromise or breach; speedy recovery or frustration.

The research question we explored is: **"Which entities do people trust when looking for cybersecurity advice and help? How does this trust change based on race?"**
Hypothesis 1: People who identify as a non-white race will show less trust in authorities like Government and Police related to cybersecurity advice.
Hypothesis 2: People who identify as a non-white race will prefer to not go to a high-end store for help.

Related Works:

In Marotzki, et.al's chapter within Computational Visualistics, Media Informatics, and Virtual Communities, two types of trust are identified, personal and systemic.[5] Personal trust refers to the trust people place in the physical dimension to individuals. Systemic trust refers to the trust people have in technology systems. The authors also

Informatics, and Virtual Communities. Bildwissenschaft, vol 11. Deutscher Universitätsverlag. https://doi.org/10.1007/978-3-322-81318-3_8.

[4] Angela D. R. Smith, Alex A. Ahmed, Adriana Alvarado Garcia, Bryan Dosono, Ihudiya Ogbonnaya-Ogburu, Yolanda Rankin, Alexandra To, and Kentaro Toyama. 2020. What's Race Got To Do With It? Engaging in Race in HCI. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–8. DOI:https://doi.org/10.1145/3334480.3375156.

[5] Marotzki, 2003.

acknowledge that no action people take is truly risk-free and more often than not occur within insufficient knowledge. Trust is key in reducing the complexity of the decision making process and in mitigating decision risks enough to overcome and "bridge" a person's ignorance in the temporal dimension. In other words, trust is critical in being able to make the best decision, with imperfect information, as quickly as possible. Additionally the authors discuss an Identity, Trust, Technology Triangle where they acknowledge the interwoven and dependent nature of the three components. Identity is referring to authentication of an entity's truthfulness in representing that they are who they proclaim to be. Our application of this academic work into our own research includes the notion of identity in the physical world carrying over into the digital world, especially within online social networks. Applying this to our earlier disinformation campaign example; Russian GRU agents were able to create credible but fake online identities to propagate their fake news with real consequences to not only US Elections but within the targeted ethnic groups.

In another related work, Ogbonnaya-Ogburu, et.al applies "Critical Race Theory for HCI."[6] In this paper, the authors propose using the core principles within Critical Race Theory developed by legal scholars in the 1970s to research within Human Computer Interactions. These authors believe that critical race theory can help advance the body of research of racism in our "socio-technical world" and improve the maturity of discourse of this topic within the academic community. The authors highlight the key tenets of critical race theory as:

- Racism is ordinary, not aberrational.
- Race and racism are socially constructed.
- Identity is intersectional.
- Those with power rarely concede it without *interest convergence.*
- Liberalism itself can hinder anti-racist progress.
- There is a uniqueness to the voice of color, and storytelling is a means for it to be heard.

Applying this to HCI, the authors encourage the academic community to acknowledge that racism is persistent and present; racism is not an "aberration" that occurs occasionally. This is one of many applications the authors make to HCI but the one we found most relevant to our endeavor. In considering how racism exists within the cybersecurity industry, we approached the question assuming that racism is pervasive and our challenge would be to narrow our field of study to a point where we could provide the most social benefit with the limited resources at our disposal.

---

[6] Ihudiya Finda Ogbonnaya-Ogburu, Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical Race Theory for HCI. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–16. DOI:https://doi.org/10.1145/3313831.3376392.

Another interesting related work we found was written by Naef and Schupp in 2009.[7] These researchers conducted trust based studies using surveys. In their study they looked beyond the traditional social based trust topic and also explored trust in institutions. The researchers were able to conclude that with enough participants the survey results were statistically significant to reach conclusions about measuring trust through a survey. We found this to be encouraging for our own study's methodology.

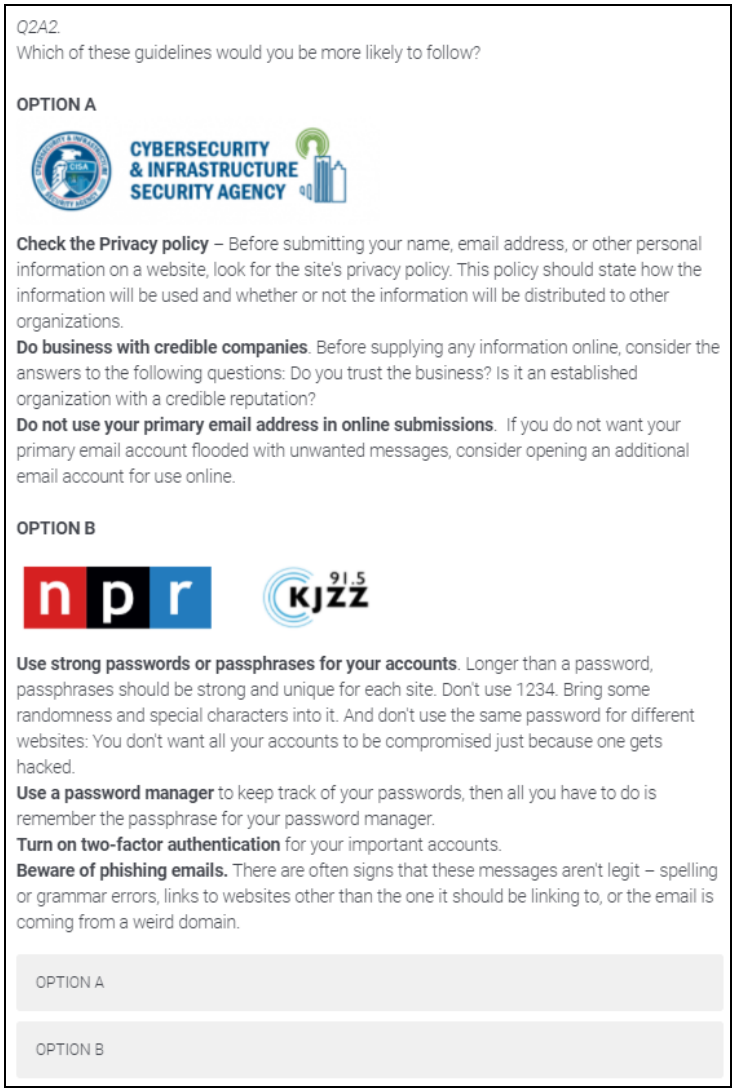
Methodology

Utilizing a survey developed on Qualtrics, we asked questions to measure the relative trust people have in various organizations' cybersecurity advice and/or help. We looked at the following sources of information or help: government (federal), police, corporations, non-profits, and friends or family. In order to evoke sentiment and see which of these sources of information people turned to most, we looked at a number of scenarios. We set up scenarios for someone receiving cybersecurity advice from various institutional sources, searching for information or help related to cybersecurity topics, needing help to regain access to their smartphone, and wanting to verify a news story. We also set up scenarios in the "real world" as a baseline to compare against cybersecurity topics. We asked what people would do after getting a wallet and phone stolen, and in a non-threatening scenario, if they would grant permission for their child to go on various field trips. Finally, we gathered information about the participants' level of technical and cybersecurity expertise, and demographic information including gender, age, employment, income, and ethnicity.

We had three iterations of friendly survey-takers, who not only took the survey but also provided feedback on comprehension of the questions. These reviews helped us finalize the survey structure as described above, focusing the language and revising the questions to their final form.

For example, we wanted to investigate whether the source of cybersecurity advice might influence someone's choice of whether to follow it. We presented two pieces of advice with a logo heading from CISA (US government agency) or from NPR (national public radio, non-profit organization). The two pieces of advice were always shown in the same order, but we randomized whether participants got the CISA header on the first advice text or the second. This question required several iterations in order to make it readable and less confusing in the survey interface.

[7] Michael Naef, Jurgen Schupp. 2009. "Measuring Trust: Experiments and Surveys in Contrast and Combination." IZA DP No. 4087. http://ftp.iza.org/dp4087.pdf.



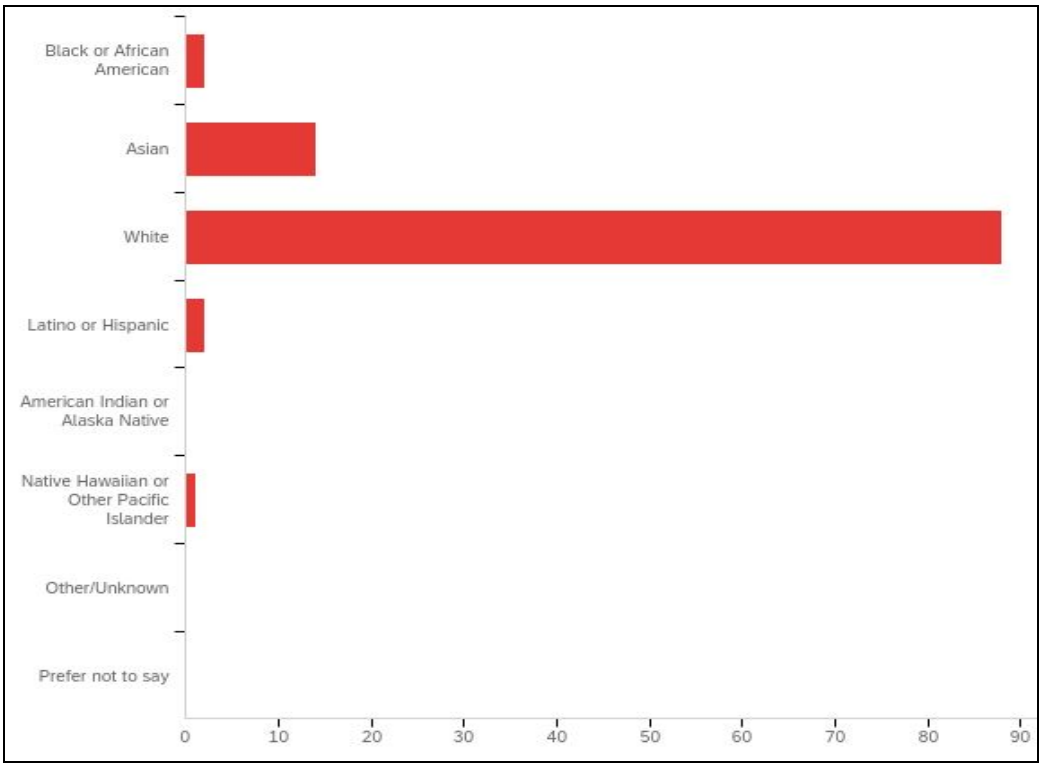
Another question we wanted to investigate was the level of comfort someone might feel having to go into a store in person in order to restore access to their smartphone. With the idea that many people of color feel distrusted in some retail stores (see “shopping while black”), we wanted to see if that would hold true for a security related topic. Initially we wanted to directly ask about the level of comfort experienced at a “fancy high-end store”, but realized that this would be too leading, and the store description was too biased. This resulted in reworking the question as a side-by-side comparison between two stores with accompanying photos that implied a higher-end experience at a mall and a more basic experience in a standalone store. We added an open-ended question to help understand why the choice was made.

For survey participants, we designed a HIT for Amazon Mechanical Turk, requesting Master Workers located in the US and HIT approval rate over 95%. We set up an initial

batch of 10 surveys for $3.20/survey, and when we confirmed we could get good results, we did a second batch of 90 at $2.50/survey. We ended up with 104 finished survey responses.

Results:

This pilot of 104 finished surveys biased male with 62 men, 41 women and 1 non-binary participants, over an age range of 24 to 74 years (average 40, stddev 10). The participants also biased toward technical and cybersecurity proficiency, with 88.5% declaring themselves proficient or higher with technology, and over half (64.4%) declaring themselves proficient or higher in cybersecurity. Unfortunately, the most biased results were ethnicity, with a very small non-white population (17.76%) including only 2 (1.9%) respondents identified as Black or African American, 14 (13%) identifying as Asian, and 2 respondents identified as Latino or Hispanic (1.9%). This means that we could not analyze our results by race.

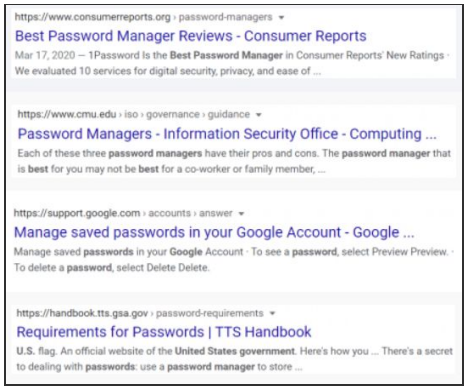


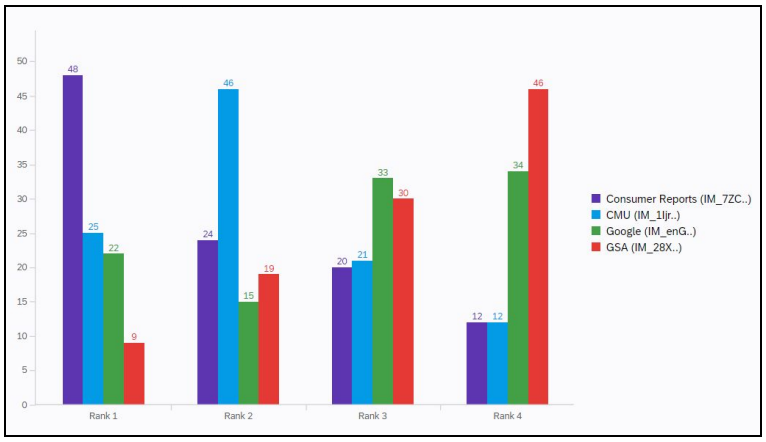
In analyzing the Cybersecurity and Infrastructure Security Agency (CISA) vs National Public Radio (NPR) cybersecurity advice question, we wanted to see if the graphic indicating the source of the advice had any influence on the selection. A chi-square test of independence showed that there was no significant association between the

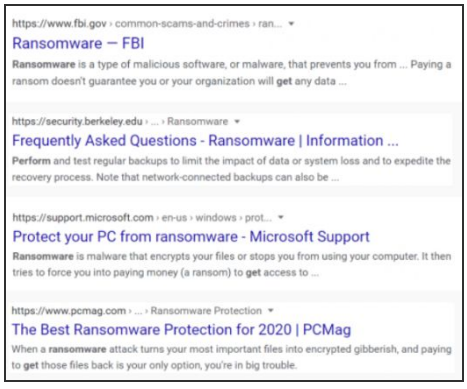
selection of OPTION A or OPTION B and whether CISA (Government) was associated with OPTION A or OPTION B, X^2 (1, N = 104) = .47, p = .49.

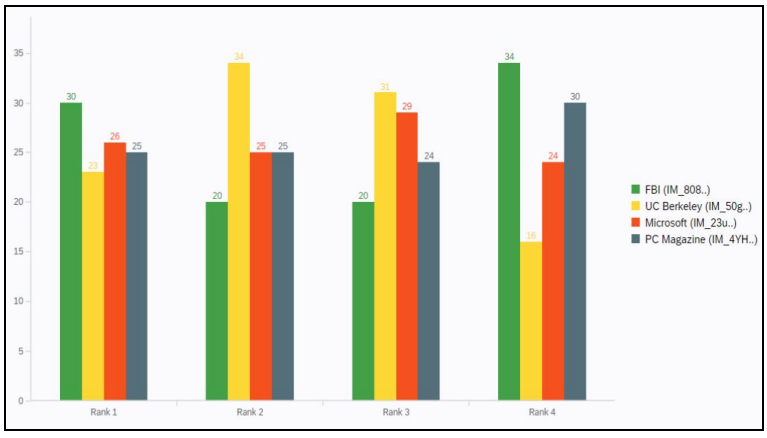
	Gov label on A	Gov label on B	*Marginal Row Totals*
OPTION A	15 (13.41) [0.19]	16 (17.59) [0.14]	31
OPTION B	30 (31.59) [0.08]	43 (41.41) [0.06]	73
Marginal Column Totals	45	59	104 (Grand Total)

Looking at the search results questions, for the password manager advice, we see a fairly consistent ordering of Consumer Reports first, followed by Carnegie-Mellon University (CMU) and Google, and ending with General Services Administration (GSA) (government). Interestingly, for the ransomware question, we found that the options were more evenly-distributed, and the FBI option was most-often selected both first and last.





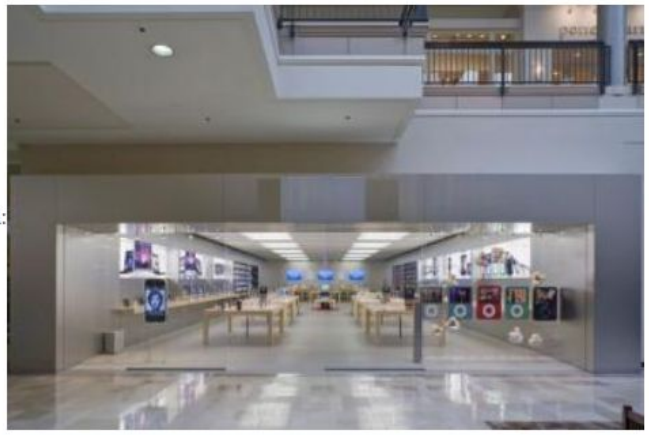




For the comparison of the fancy mall store against the standalone store, we found that the standalone store was overwhelmingly preferred, by 75 of the participants. We informally coded the open-ended responses to get an idea of what participants said

about the two options. These are the positive and negative sentiments expressed about why each store was chosen, displayed as a word cloud:

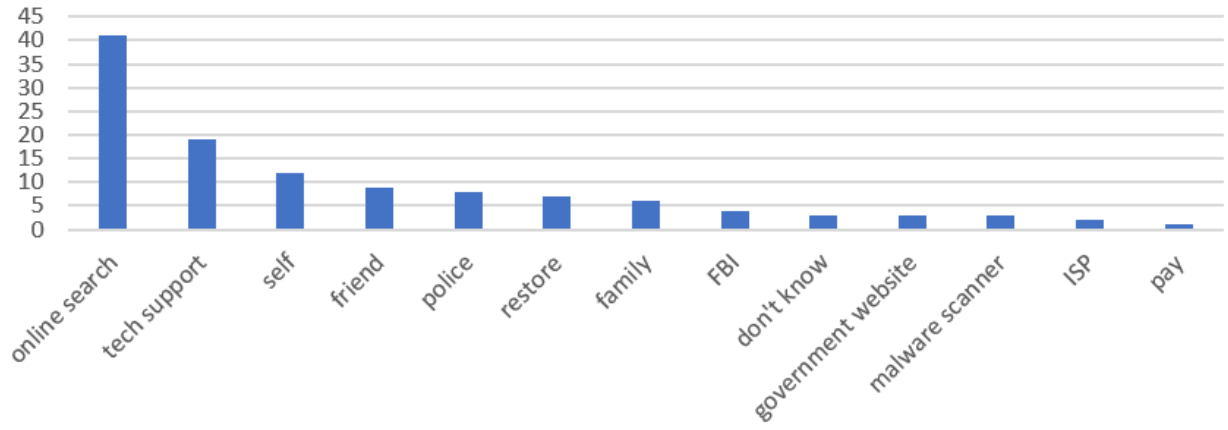
Store at the mall:



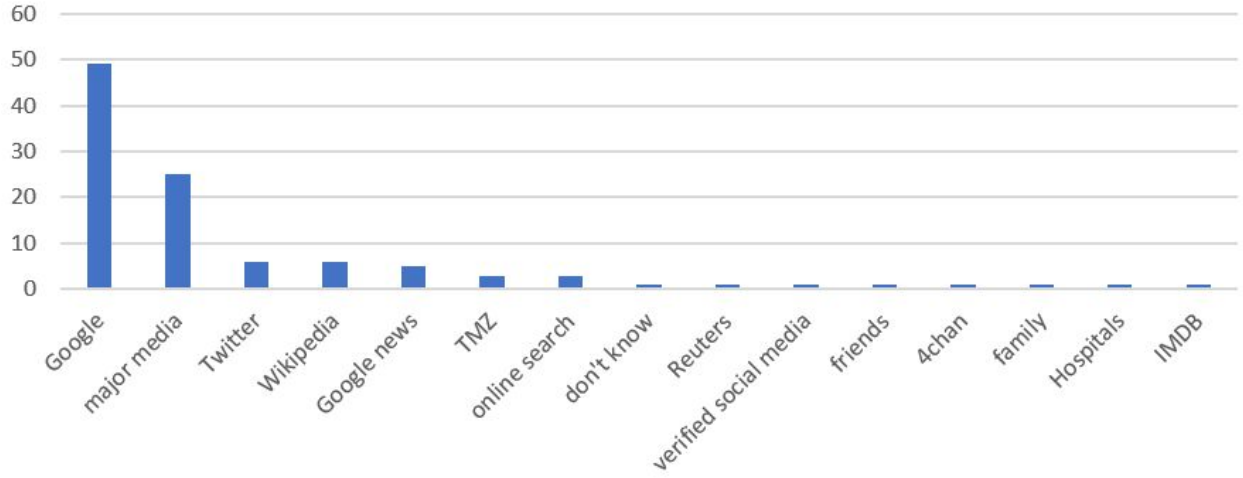
Standalone store:

We were curious if this preference for the standalone store was influenced by gender, with men stereotypically preferring to not go to the mall. Analyzing by gender, 12/41 (29.3%) of women prefer the mall store, compared to 17/62 (27.4%) of men. A chi-square test of independence showed that there was no significant association between the selection of the store by gender, X^2 (1, N = 103) = 0.04, p = .83.

After coding the open responses about where people would go for help if their system got infected with ransomware, the results showed that most people would try to resolve the issue themselves, or check with an internet search how to resolve the problem. Note that there are more than 104 selections here as some responses included more than one option (like “myself restoring my computer” got coded as both “self” and “restore”).



After coding the open responses about where people would go to verify a news story seen on social media, it's heartening to see that most people would go to Google and major news media sources to verify a story on social media.



Discussion:

While our survey results included interesting trends, we could not use them to definitively answer our research question. Even with 104 completed surveys, there wasn't statistical significance in any of our relevant results. The best we can do in discussing the results is determining how we could refine our survey's scope and questions to achieve the statistical significance needed to draw meaningful conclusions.

First, we were surprised to see such a heavy bias towards participants identifying as White, male, and tech savvy. Perhaps this is a reflection of the Mechanical Turk (MTurk) workforce overall or it could be heavily influenced by the timing of our survey's release into the MTurk tasks list. If we were to continue research on this topic, we would recruit participants outside of the MTurk system.

In the rank ordering survey question for password manager and ransomware, we recognize that the headline and subtext of each search result could influence the results more than the actual source. In future iterations of this survey we could create 2 sets of search results, one including the source and another with the source removed. Using this we may be able to confirm or deny the impact of the subtext and headline versus the impact of the source itself. We have similar observations in our CISA versus NPR survey question. Respondents seemed to focus less on the source of the information itself and preferred the actual advice provided in Option B. For future studies we would once again provide half of the respondents with just the text based advice and the other half with the text and source indication.

While we can continue to analyze the data, we would like to also share some of the key lessons learned from this pilot and overall endeavor to understand how systemic racism manifests within cybersecurity. The first lesson is that “smaller bites equals greater impact.” In other words, the scope of our initial research study was far too large to feasibly study at once. Our group initially attempted to understand how racism could manifest and impact the effective use of humans and chatbots. After much advice and consultation from our professors, we were able to pivot towards a research question offering a much clearer connection to the social benefit we hoped to achieve. Consequently, our group began to hone in on trust different racial groups would have in sources of cybersecurity advice. After completing our pilot survey, we see even more opportunity to further refine our scope. In this study we looked at both cybersecurity scenarios and sources of advice. In future iterations, we would further narrow our scope by looking at just cybersecurity scenarios OR sources of advice. Based on our pilot results, we are confident the body of work and knowledge to uncover in a refined setting would lead towards meaningful results and net positive social benefits.

As we covered in our introduction, trust is necessary for people to make quick decisions even with insufficient knowledge. Cybersecurity is an ever evolving field that promises to become more and more technical. However, cybersecurity is now a critical component in ensuring that everyone’s daily lives can continue uninterrupted and unimpeded by malicious actors. In being able to cover this knowledge gap, HCI and cybersecurity professionals should explore who communities trust for information and advice. We will also need to understand that race plays a role in every piece of technology we produce. Combining our improved understanding of trust at the intersection of race and cybersecurity will help to ensure an equitable and secure socio-technical world.

Acknowledgements:

Cristian Bravo-Lillo and **Stuart Schechter** for assisting us throughout the duration of this study. They provided our team with guidance and support in all stages but was especially helpful in guiding us towards a viable research question exploring the intersection of race and cybersecurity. We initially struggled with finding a suitable research question and initially pursued understanding how systemic racism would manifest itself within chatbots. This proved to be too large for the scope of this course, Cristian and Stuart spent many additional hours with us to hone in our studies focus.

Maritza Johnson helped provide additional input and guidance on how we could ask questions and uncover additional knowledge when looking at trust networks in the cybersecurity realm.

Our classmates: Alana Franklin, Atefeh Namvaryshad and Nestor Catano for providing us with additional feedback, thoughts, and support throughout the course.

References:

Marotzki W., Dittmann J., Lesske F. (2003) Virtual Communities: Trust, Identity, Participation, and Technology. In: Schneider J., Strothotte T., Marotzki W. (eds) Computational Visualistics, Media Informatics, and Virtual Communities. Bildwissenschaft, vol 11. Deutscher Universitätsverlag. https://doi.org/10.1007/978-3-322-81318-3_8.

Naef, Michael, Jurgen Schupp. 2009. “Measuring Trust: Experiments and Surveys in Contrast and Combination.” IZA DP No. 4087. http://ftp.iza.org/dp4087.pdf.

Ogbonnaya-Ogburu, Ihudiya Finda; Angela D.R. Smith, Alexandra To, and Kentaro Toyama. 2020. Critical Race Theory for HCI. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–16. DOI:https://doi.org/10.1145/3313831.3376392.

Smith,Angela D. R., Alex A. Ahmed, Adriana Alvarado Garcia, Bryan Dosono, Ihudiya Ogbonnaya-Ogburu, Yolanda Rankin, Alexandra To, and Kentaro Toyama. 2020. What's Race Got To Do With It? Engaging in Race in HCI. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20). Association for Computing Machinery, New York, NY, USA, 1–8. DOI:https://doi.org/10.1145/3334480.3375156.

Stewart, Camille. “Systemic Racism Is a Cybersecurity Threat,” June 16, 2020. https://www.cfr.org/blog/systemic-racism-cybersecurity-threat.

U.S. Senate, 116th Congress, 1st Session, “Russion Active Measures Campaigns and Interference in the 2016 U.S. Election,” August 18, 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.