Johns Hopkins University

Information Security Institute

Maryland Resident Cybersecurity Awareness and Practices PILOT Survey: Preliminary Report

Anton Dahbura, Joseph Carrigan, Jamie Stelnik and Mohammed Khalid

Contact Information: Anton.Dahbura@jhu.edu

Abstract: We conducted a pilot survey on the cybersecurity habits and knowledge of Maryland residents using Amazon's MTurk service. We collected over 500 valid responses from MTurk workers in Maryland and analyzed the results. Key findings include the following: A large proportion of Marylanders have been the victims of online scams where they experienced a financial loss. Marylanders seem overconfident in their cybersecurity knowledge. One in five Marylanders admit to using the same password for most of their online accounts. In this report we discuss the survey and its methods, analyze the compiled results of the survey, and recommend further, more rigorous research in this area.

Funding for this work was provided by
the National Cryptologic Foundation and
the Johns Hopkins University Information Security Institute.

October 14, 2023

Contents

List of Figures

List of Tables

Chapter 1

Acknowledgements

The Maryland Resident Cybersecurity Awareness and Practices survey would not have been possible without the work and guidance of many individuals from across the Johns Hopkins and Maryland communities. We want to thank each of them for their input, guidance, and commitment to inclusive excellence at The Johns Hopkins University Information Security Institute.

Chapter 2

Introduction

2.1 Background

The Maryland Resident Cybersecurity Awareness and Practices Survey was conducted by members of the Johns Hopkins University Information Security Institute (ISI) in order to become more informed about Maryland residents' general knowledge of cybersecurity, their cybersecurity practices, and the impact of cyber scams on their lives. The survey allows participants to respond regarding their personal practices or their practices at their work, without distinguishing between the two.

2.2 Objectives

The primary objective of this pilot survey is to perform a preliminary assessment of the cybersecurity knowledge and habits of Maryland residents. The results of this survey are intended to guide the direction of future research into the topic area. Future surveys should be more formal and use the lessons learned in this survey to focus more on areas that emerge as interesting to future researchers while still, more importantly, pertinent to Maryland residents.

2.3 Organization of the report

This report is organized into five chapters. Chapter 1 is the Acknowledgements. Chapter 2 is the Introduction. The Introduction goes into background of the project, objectives, and organization of the report. Chapter 3 is the Methodology. The methodology describes MTurk, the Census Data used, and how the survey data was analyzed. Chapter 4 contains the Results of the survey. Our results are split into 6 key sections: demographics, cybersecurity and computer knowledge, cybersecurity hygiene, security questions, and victim scamming. The final chapter, Chapter 5, contains discussions of and conclusions taken from the results, including participants' overconfidence in cybersecurity knowledge, high victim rate of online scams, password reuse, and ignorance about data breaches.

Following the five chapters, there are three appendices. Appendix A shows the one-dimensional graphs of survey data, Appendix B shows the Maryland 2020 census data compared to the survey data, and Appendix C lists the survey questions asked to participants.

Chapter 3

Methodology

3.1 MTurk

3.1.1 Introduction to Amazon Mechanical Turk

The Amazon Mechanical Turk (MTurk) platform was used to recruit participants, conduct the survey, and gather results. MTurk is a 'crowdsourcing' website with which businesses can hire remotely located "crowdworkers" to perform discrete on-demand tasks. Employers (known as requesters) post jobs known as Human Intelligence Tasks (HITs), such as identifying specific content in an image or video, writing product descriptions, or answering survey questions. Workers, colloquially known as Turkers or crowdworkers, browse among existing jobs and complete them in exchange for a fee set by the employer. [Wikipedia]

3.1.2 Survey Details on MTurk

The survey was conducted on MTurk from October 2022 through February 2023. 549 participants completed the survey and were paid $5 each. The survey was listed as "Survey About Your Cybersecurity Habits" and participants were told that the survey would require approximately 10 minutes to complete. Funding for the survey fees were provided by the National Cryptologic Foundation and ISI.

The participants were asked to answer 31 questions as seen in Appendix C.

3.1.3 Analysis of Respondent Authenticity

For data reliability, we performed an extensive analysis to address concerns about respondent authenticity. Considering prior worries about bots in MTurk respondents, our analysis aimed to boost data quality.

We checked for duplicate IP addresses, verified if IP addresses and GPS locations were in the United States, and made sure respondents' birth years matched their chosen age ranges.

These results, which include a relatively low number of cases where discrepancies were observed among the survey respondents, serve to enhance our confidence in the authenticity of the survey participants. The fact that only 33 respondents had inconsistencies in their selected age ranges, 79 had non-U.S. IP addresses, and 116 exhibited duplicate IP addresses is encouraging.

While these findings do suggest potential issues, their relatively limited occurrence suggests that the majority of our survey data is reliable and provided by genuine participants. We also consider Amazon's identity verification, adding an extra layer of result integrity.

3.2 Census Data

2020 Maryland Census Data was used in order to gain census demographic information pertaining to Maryland Counties by United States Census Bureau (2023) and Maryland Department of Planning (2022).

3.3 Analysis of Data

The survey data was analyzed using Python through Jupyter Notebook. Both graphs and tables were created with the survey data and census data. The data was visualized through bar graphs and crosstabs. Crosstabs visualize the frequency distribution of two different survey questions. One-dimensional bar graphs were created to visualize how many participants chose each answer for a question. Dual-axis bar graphs were used to compare these survey ratios to the census data ratios. Finally, crosstabs were used to create two-dimensional tables, comparing each question to each other by seeing how many participants answered each combination of answers.

Chapter 4

Results

4.1 Demographics

The demographics taken from our survey included questions about age, location, and education level.

In the first question, participants were asked to pick the age range which corresponds to their current age: 18-24, 25-34, 35-44, 45-54, 55-64, and 65 years and older. As can be seen in Figure 4.1, most of the survey participants were between the ages of 25 and 44. When comparing the number of survey participants in each age range to the number of Maryland residents in each age range using Maryland 2020 census data, Figure 4.2 was created. This figure highlights that while most age ranges are evenly represented in the state of Maryland, this survey highly favored the younger age groups.

This concentration towards middle age groups was not unexpected as we were aware that MTurk workers' ages would probably be skewed this way. However, this will impact the results for the rest of the survey, as there is more evidence to support the results for ages 25-44 than, say, 65 years and older, where there were only 12 respondents.

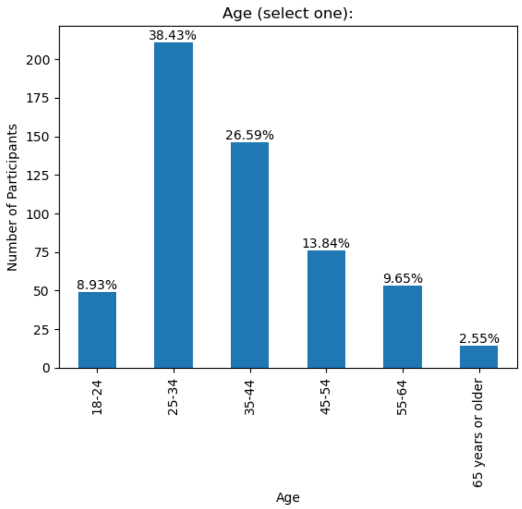


Figure 4.1: Age of Maryland Survey Participants

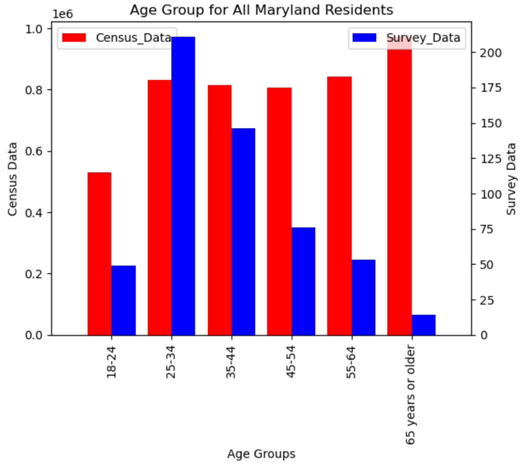


Figure 4.2: Age of Survey Participants In Comparison to Maryland 2020 Census

The second question had survey participants mark their county of residence. This data can be seen in Figure 4.3. In order to visualize this data more efficiently, we have grouped these counties into their respective regions, as seen in Table 4.1. This survey data grouped into regions of residence is shown in Figure 4.4. It is interesting to note that the Capital Region is underrepresented in the survey, while Western Maryland is overrepresented (see Figure 4.5). While not pertinent to the research done in this report, the increase in participants from Western Maryland along with the decrease in the Capital Region was surprising to see.

Table 4.1: Maryland Counties by Region

Region	**Counties**
Capital Region	Frederick County, Montgomery County, Prince George's County
Central Maryland	Anne Arundel County, Baltimore City, Baltimore County, Carroll County, Harford County, Howard County
Southern Maryland	Calvert County, Charles County, St. Mary's County
Eastern Shore	Caroline County, Cecil County, Dorchester County, Kent County, Queen Anne's County, Somerset County, Talbot County, Wicomico County, Worcester County
Western Maryland	Allegany County, Garrett County, Washington County

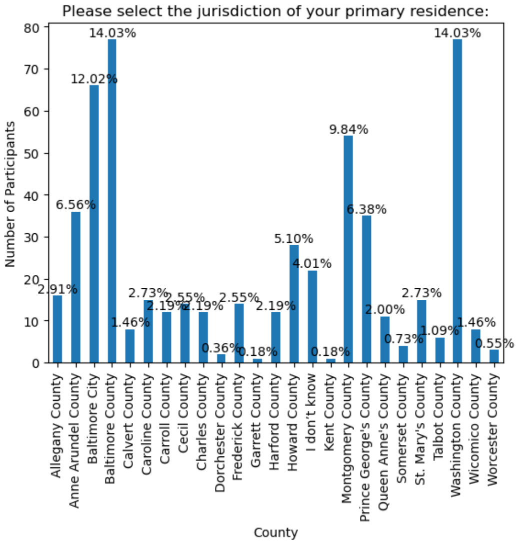


Figure 4.3: County of Residence of Maryland Survey Participants

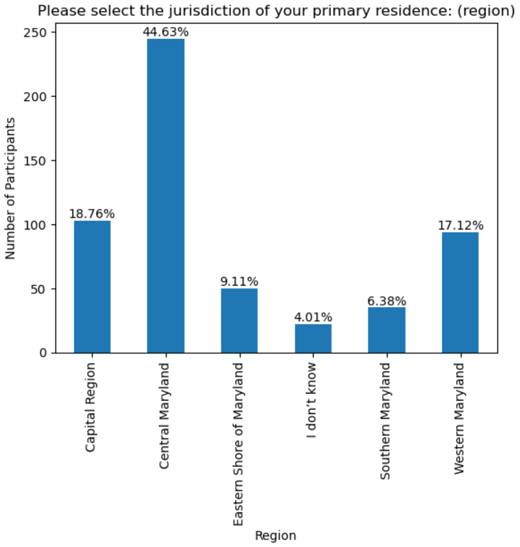


Figure 4.4: Region of Residence of Maryland Survey Participants

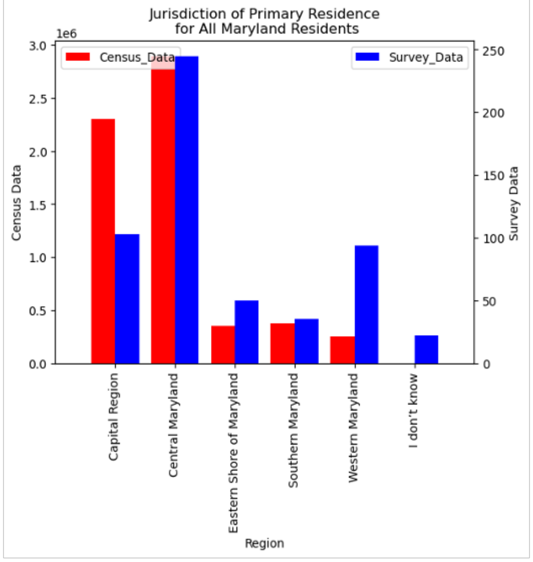


Figure 4.5: Region Residence of Survey Participants In Comparison to Maryland 2020 Census

In the final demographic question, survey participants were asked about their highest level of education as seen in Figure 4.6. It is clear when comparing Figure 4.6 and Figure 4.7 that a somewhat more highly educated group of people from Maryland took this survey. The figures for non-high school graduates, high school graduates, some college, and associates degrees are represented fairly in each region when compared to census data (Figures 4.8, 4.9, 4.10, 4.11). However, for both bachelor's and graduate degrees, there is higher representation from Western Maryland than expected from census data, as well as lower representation from the Capital Region (Figures 4.12, 4.13). So it seems as if there were more highly-educated people in Western Maryland working on MTurk, and fewer in the Capital Region.

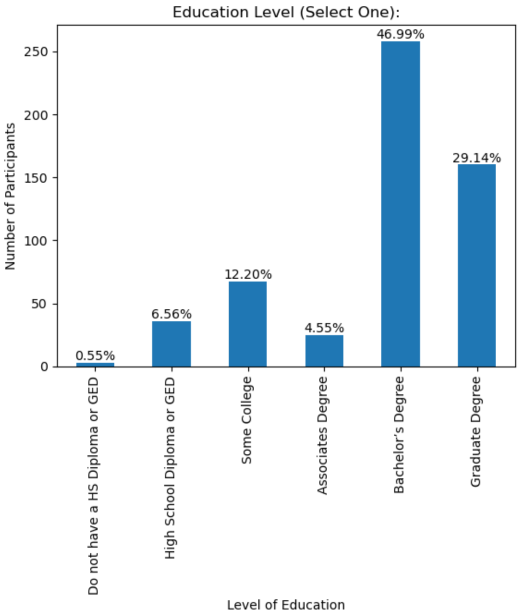


Figure 4.6: Highest Education Level of Maryland Survey Participants

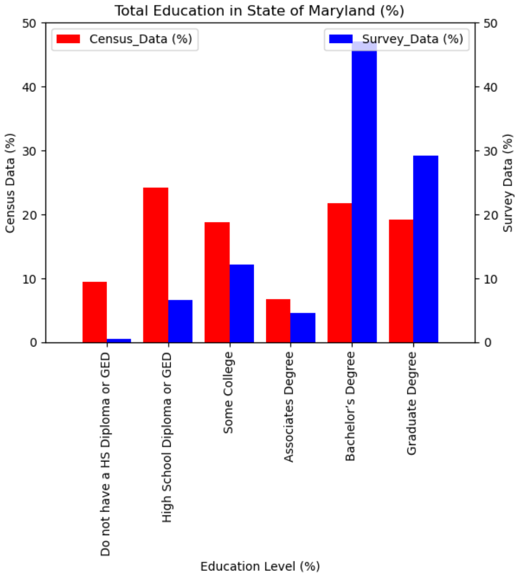


Figure 4.7: Education Level of Survey Participants In Comparison to Maryland 2020 Census

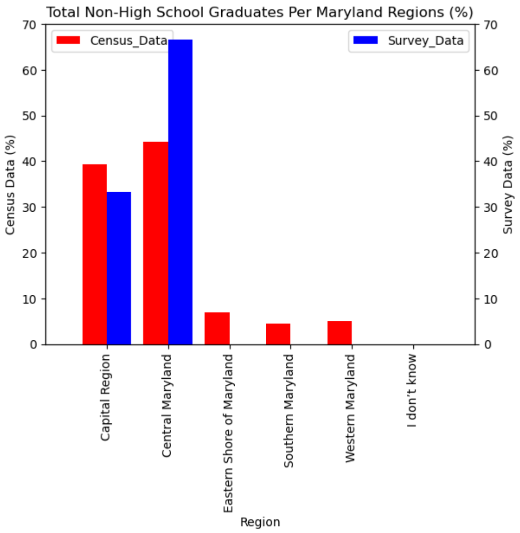


Figure 4.8: Survey Participants Without High School Graduation In Comparison to Maryland 2020 Census

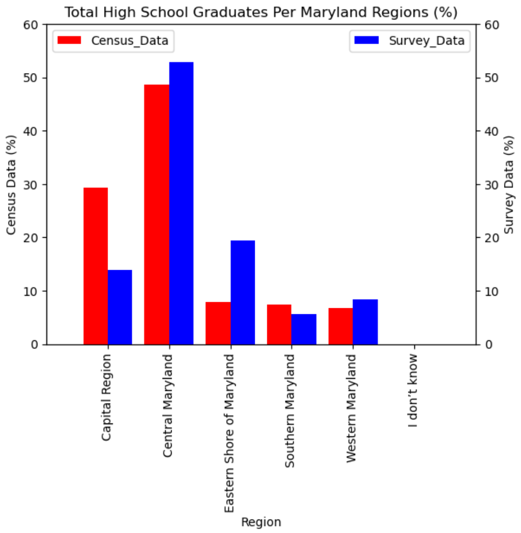


Figure 4.9: Survey Participants With High School Graduation In Comparison to Maryland 2020 Census

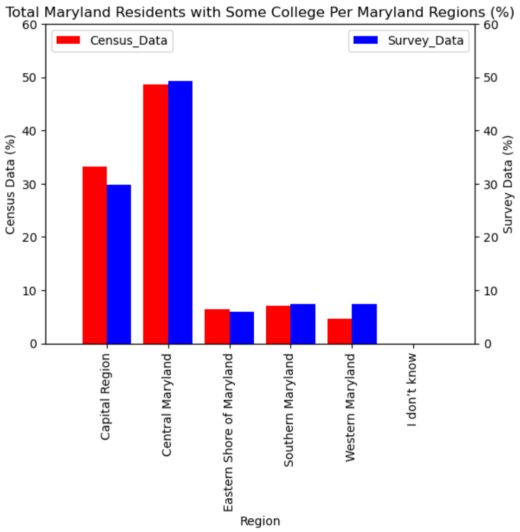


Figure 4.10: Survey Participants With Some College In Comparison to Maryland 2020 Census

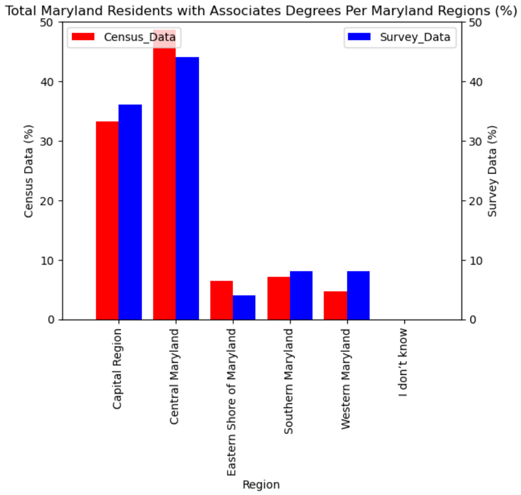


Figure 4.11: Survey Participants With Associates Degree In Comparison to Maryland 2020 Census

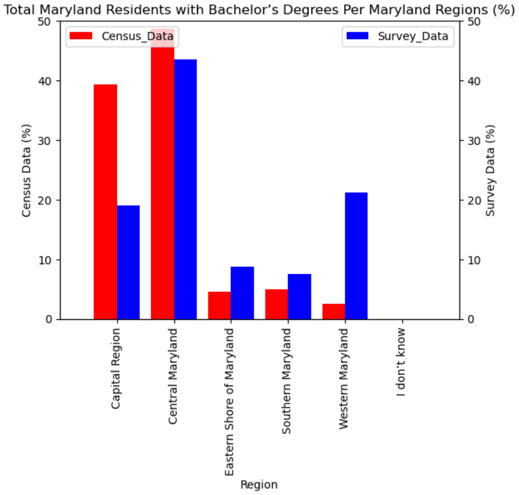


Figure 4.12: Survey Participants With Bachelor's Degree In Comparison to Maryland 2020 Census

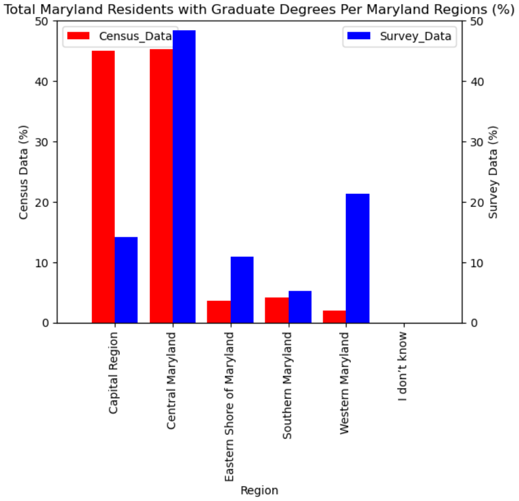


Figure 4.13: Survey Participants With Graduate Degree In Comparison to Maryland 2020 Census

4.2 Participants' Cybersecurity and Computer Knowledge

Participants were asked to rate their confidence in computer skills and cybersecurity knowledge on a five point scale of: strongly disagree, somewhat disagree, neither agree nor disagree, somewhat agree, and strongly agree. Over 85% of participants were somewhat or strongly confident in their computer skills, as seen in Figure 4.14. Around 75% of participants believed they were knowledgeable about cybersecurity, as seen in Figure 4.15. Therefore, we can assume that the participants of this survey are people that felt they were confident about their computer skills and knowledgeable about cybersecurity.

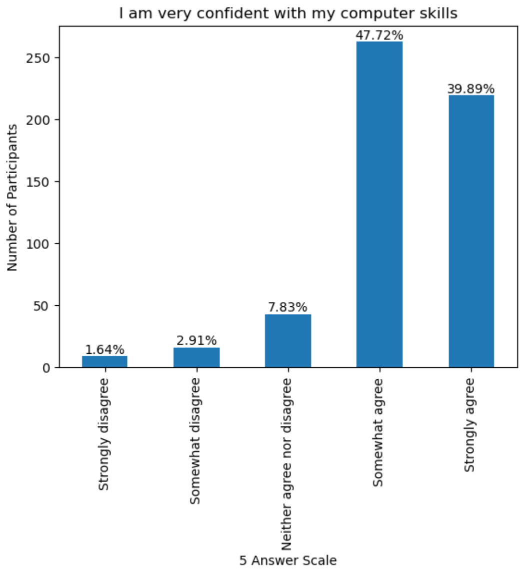


Figure 4.14: Participant Confidence With Computer Skills

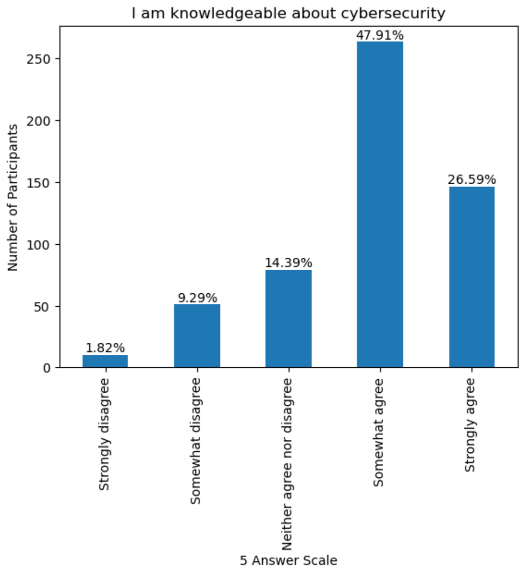


Figure 4.15: Participant Confidence with Cybersecurity Knowledge

4.3 Participants' Security Training

When considering another survey question relating to the most recent time the participant had gone through security training, it seems as though many people claim that they have received some form of security awareness training. 67% of participants claimed to receive this training within the past year. This can be seen in Figure 4.16.

One question we considered when seeing how many participants had received security trainingw was why these participants had to go through training. Did they go through training in response to being scammed? Or, were they working professionals who had to go through training as new hires?

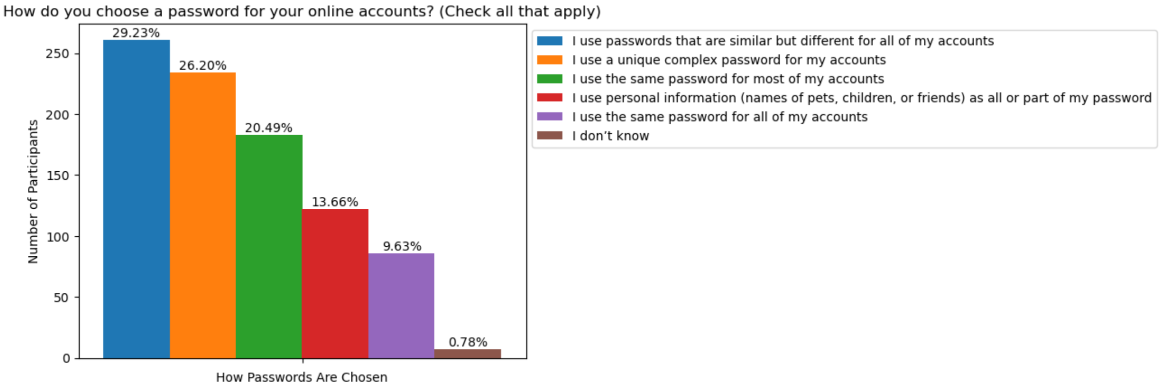


Figure 4.16: Participants' Most Recent Security Training

4.4 Participants' Cybersecurity Hygiene Practices

4.4.1 Data Backups

The first question concerning participants' cybersecurity hygiene practices questions how they back up their data, in the "check all that apply" format. As seen in Figure 4.17, almost 40% of participants said that they use a cloud service. Further, only 4% of participants said that they do not back up their data or do not know how they back up their data.

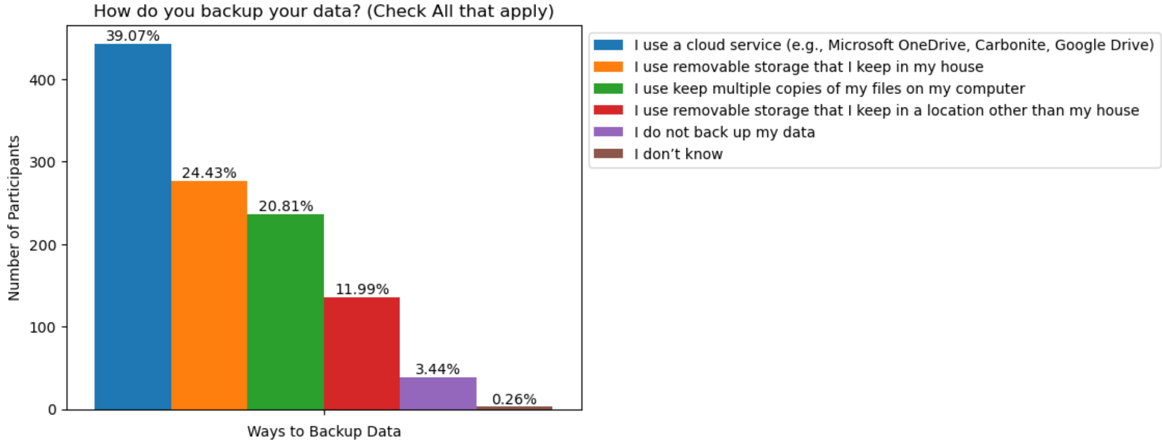


Figure 4.17: Ways Participants Back Up Their Data

Secondly, participants were asked how often they backed up their data. This was also a "check all that apply" question where participants could check weekly, monthly, continuously, daily, or that they don't back up their data. As seen in Figure 4.18, most participants (around 75%) checked that they did back up their data either weekly, monthly, continuously, or daily.

From these first two hygienic questions, we can infer that most participants are backing up their data, and doing so frequently.

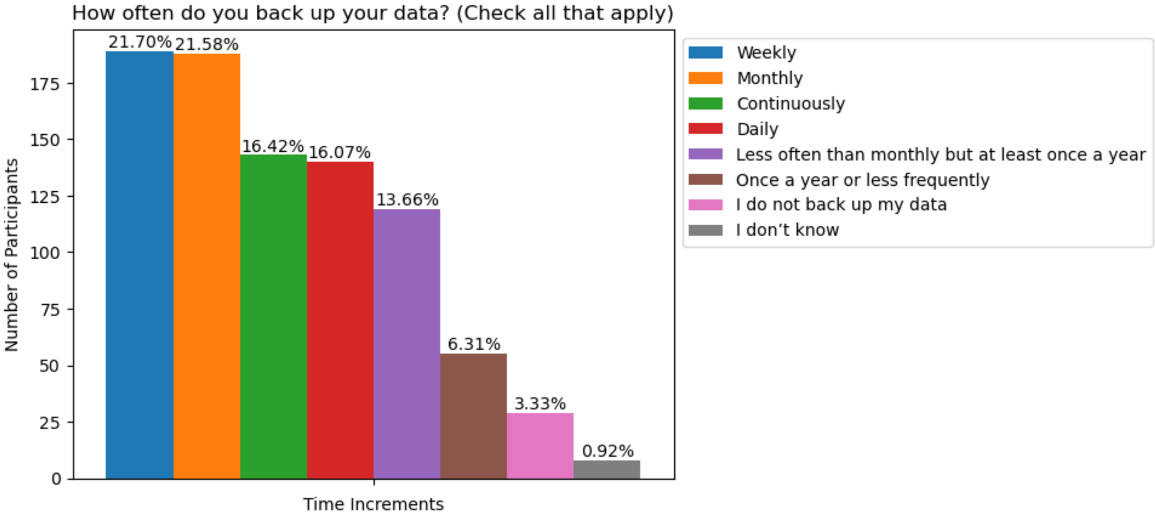


Figure 4.18: How Often Participants Back Up Their Data

Third, participants were asked for the last time they made sure their backups were valid. Over 90% of the participants claim to have checked their backups. around 44% of people claim that they've checked within the past week. This is seen in Figure 4.19.

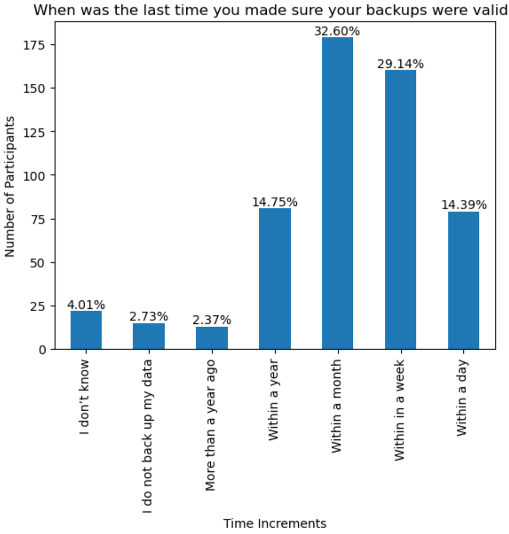


Figure 4.19: How Often Participants Check That Their Data is Backed Up

4.4.2 Multifactor Authentication

When asked about when and how they use multifactor authentication, around 6% participants said they don't use it while 3% said they do not know whether they use it. This is a very low percentage of participants, as we can see in Figure 4.20. 35% of the participants said that they use messages sent to their devices for multifactor authentication. It is interesting that Figure 4.21, the question directly following, has a different number of participants answering "I do not use multifactor authentication" and "I don't know." While this difference is small (3.73%), it is interesting to point out.

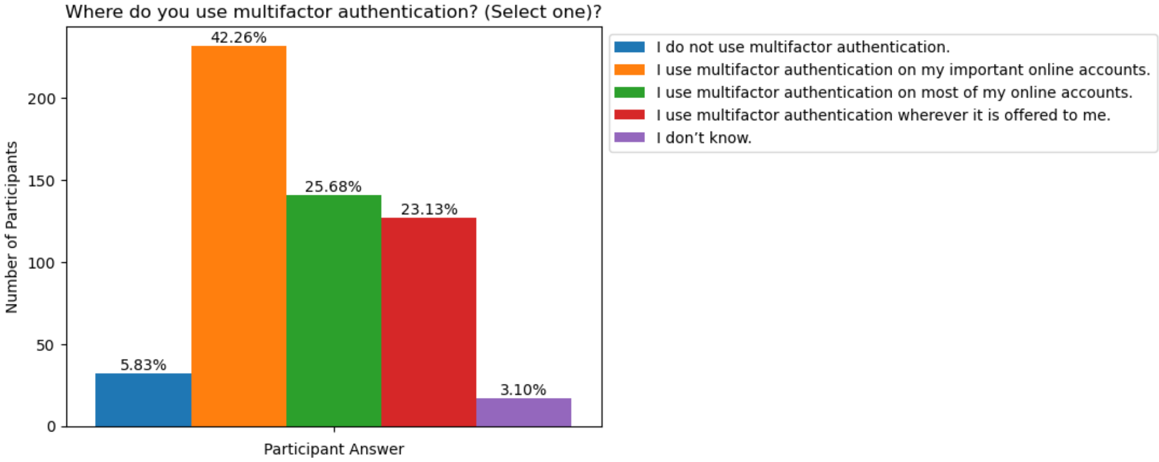


Figure 4.20: Where Participants Use Multifactor Authentication

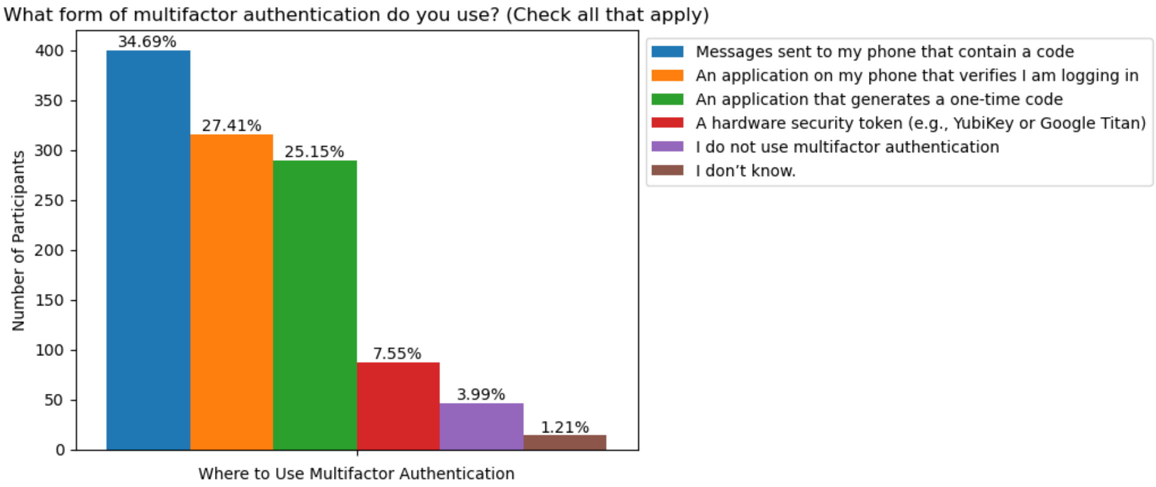


Figure 4.21: How Participants Use Multifactor Authentication

4.4.3 Passwords

Similarly, participants were asked how they choose passwords for their online accounts. In Figure 4.16, over 30% responded that they use the same password for most or all of their accounts. The other respondents either use personal information to create their passwords or use similar passwords for their accounts. As seen in Figure 4.22, participants claim they remember them or write them down. Less than 30% use a password manager.

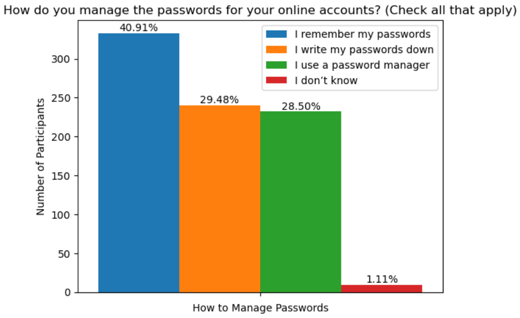


Figure 4.22: How Participants Manage Their Passwords

4.5 Security Questions

There were four questions in the survey that asked participants to answer 'quiz' questions related to common cybersecurity terms. The first question asked participants to define Social Engineering. Only 25% of participants picked the correct choice. The second question asked participants to define Spear Phishing, which had almost a 50% correct answer rate. Third, participants correctly defined Phishing with a 62% correct answer rate. Finally, over 70% of the participants correctly defined Multifactor Authentication.

The four questions in the survey are seen in the figures below: 4.23, 4.24, 4.25, 4.26

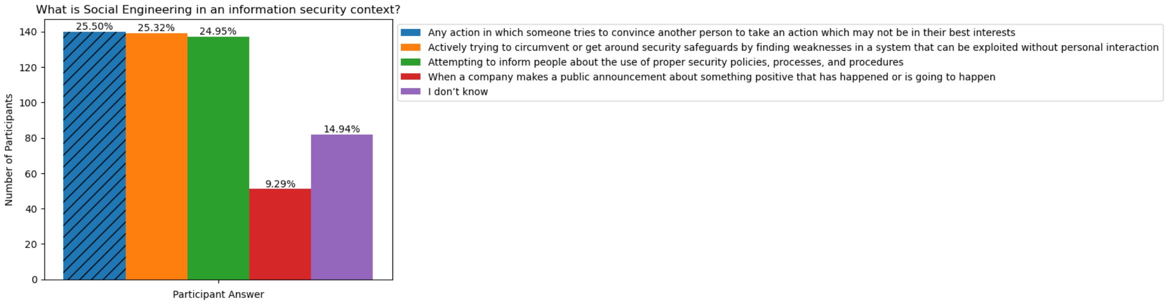


Figure 4.23: Participant Answers to "What is Social Engineering"

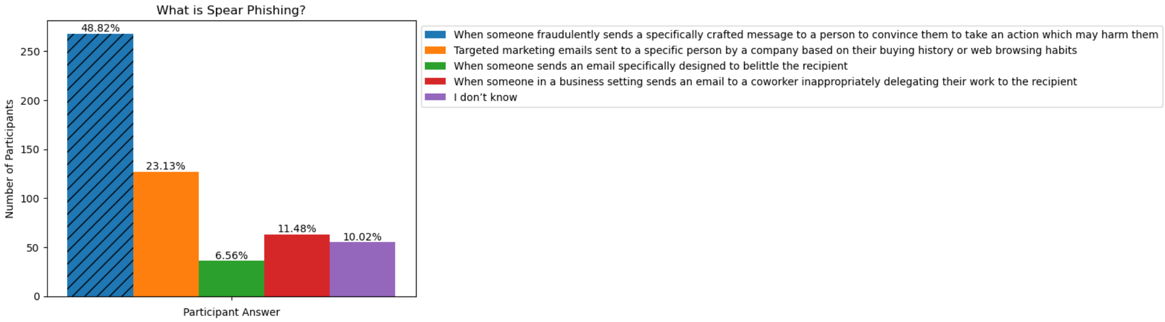


Figure 4.24: Participant Answers to "What is Spear Phishing"

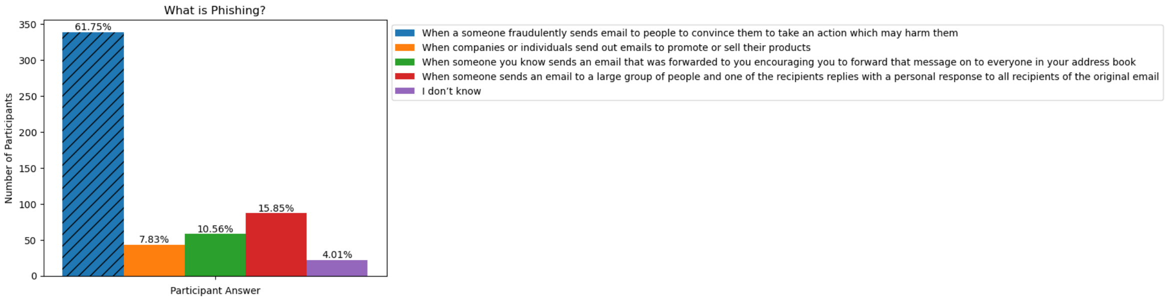


Figure 4.25: Participant Answers to "What is Phishing"

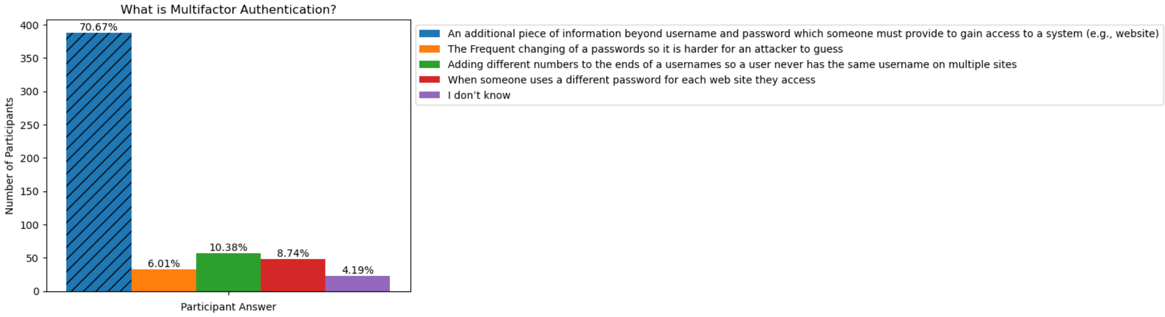


Figure 4.26: Participant Answers to "What is Multifactor Authentication"

Each participant was given a score of 0-4, representing the number of the previous four security questions they answered correctly. As seen in figure 4.27, only 14.03% of participants got all four of these questions correct. 12% of participants didn't get any of the questions correct. Over 60% of participants got two or fewer questions correct out of four. This was very surprising and will be discussed more in Chapter 5.

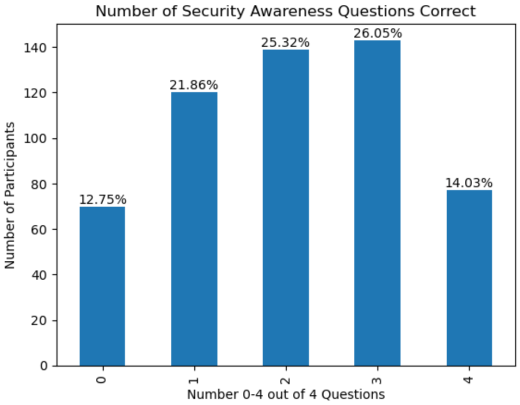
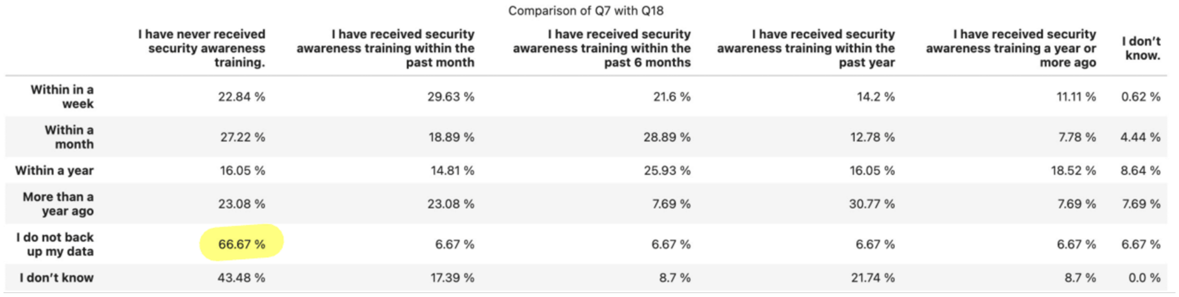


Figure 4.27: Participant Correct Answers to Knowledge Questions

4.5.1 Security Questions as a Function of Security Training

In the following Table 4.28, participants who did not back up their data were much more likely to never have received security training. See Figure 4.28. This emphasizes the fact that participants who have backed up their data are also much more likely to have had security training in the past. While this does not show any causative relationship, it does show a correlation between backing up data, which is recommended, and being trained in security.



Comparison of Q7 with Q18

	I have never received security awareness training.	I have received security awareness training within the past month	I have received security awareness training within the past 6 months	I have received security awareness training within the past year	I have received security awareness training a year or more ago	I don't know.
Within in a week	22.84 %	29.63 %	21.6 %	14.2 %	11.11 %	0.62 %
Within a month	27.22 %	18.89 %	28.89 %	12.78 %	7.78 %	4.44 %
Within a year	16.05 %	14.81 %	25.93 %	16.05 %	18.52 %	8.64 %
More than a year ago	23.08 %	23.08 %	7.69 %	30.77 %	7.69 %	7.69 %
I do not back up my data	66.67 %	6.67 %	6.67 %	6.67 %	6.67 %	6.67 %
I don't know	43.48 %	17.39 %	8.7 %	21.74 %	8.7 %	0.0 %

Figure 4.28: Relation Between Participant Correct Answers and Most Recent Security Training

4.6 Victim Scamming

Almost 20% of participants said they had been a victim of ransomware. This is over 100 of the participants (see Figure 4.29). This is an extremely high number that especially surprised us.

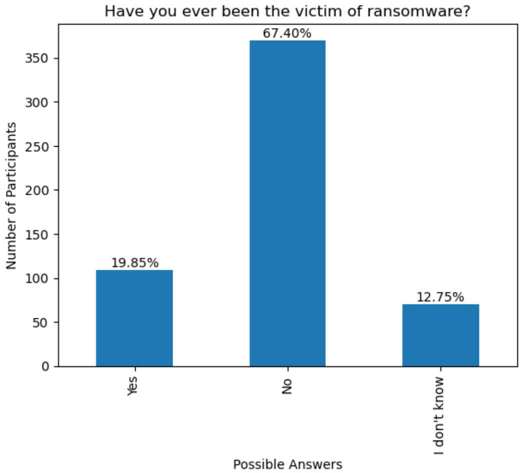


Figure 4.29: Have Participants Ever Been Victims of Ransomware?

It is widely known that almost everyone has had their personal information disclosed to someone somewhere. However, only 45% of participants answered "Yes" to the question of whether their personal information had been disclosed to unauthorized people. See Figure 4.30.

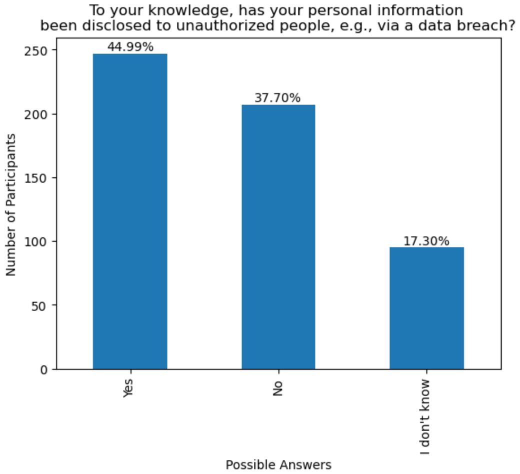


Figure 4.30: Has Participants' Information Ever Been Disclosed to Unauthorized People?

Over 20% of participants said that they had been a victim of an online scam where they lost any amount of money. Furthermore, 6% of participants said that they didn't even know whether they had been a victim. See Figure 4.31.

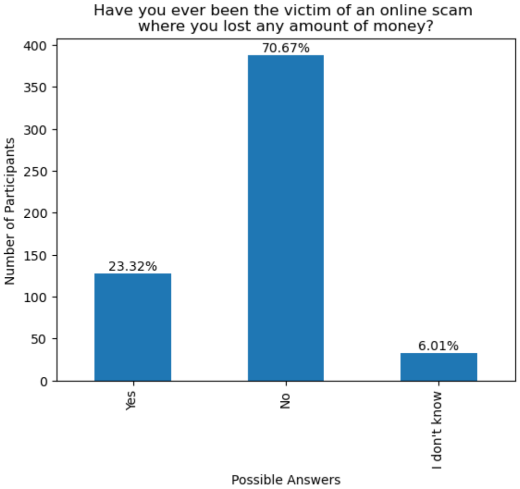


Figure 4.31: Have Participants Ever Been The Victim Of An Online Scam Where They Have Lost Money?

According to the data, the 549 participants of this survey were scammed out of $436,000. Extrapolating this amount to all Maryland residents, the 4.7 million residents of Maryland may have lost as much as $3.8 billion in on-line scams (see Figure 4.32).

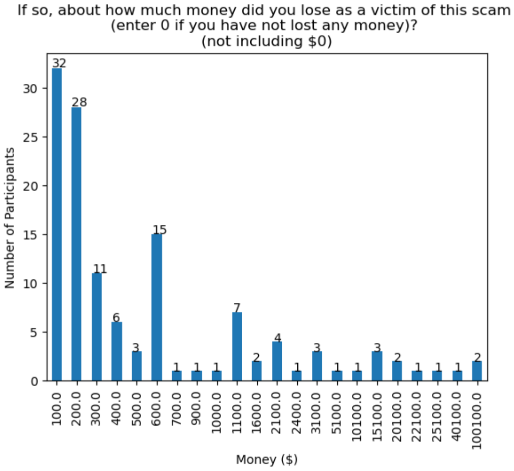


Figure 4.32: Amount that Participants Have Been Scammed Out of (Not Including $0)

In a response to whether participants have been phoned by scammers, around 63% of participants answered "Yes." See Figure 4.33. This extremely high number also surprised us.

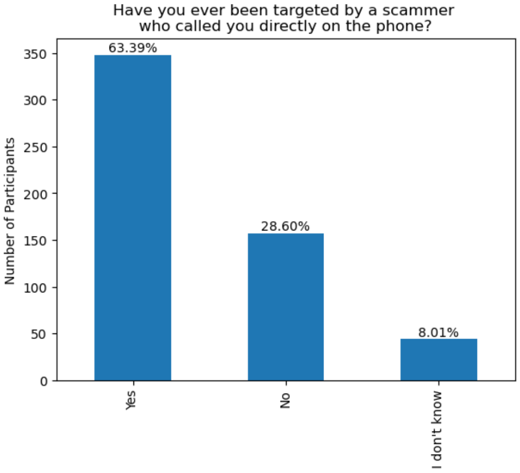


Figure 4.33: Have Participants Ever Been Scammed On the Phone?

Almost 25% of people have had their online accounts hijacked. See Figure 4.34.

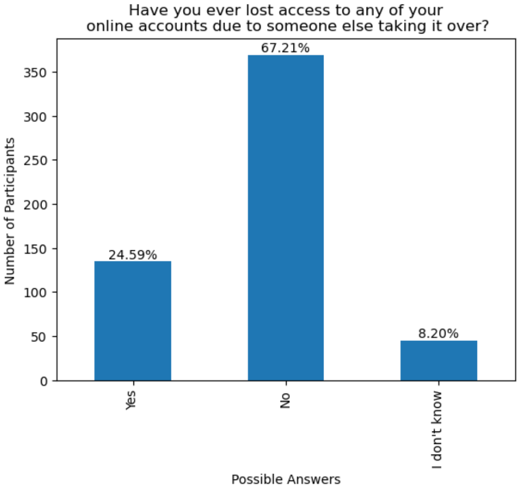


Figure 4.34: Have Participants Ever Had Their Online Accounts Hijacked?

56% of participants said they have recieved a email pretending to be a financial institution. See Figure 4.35.

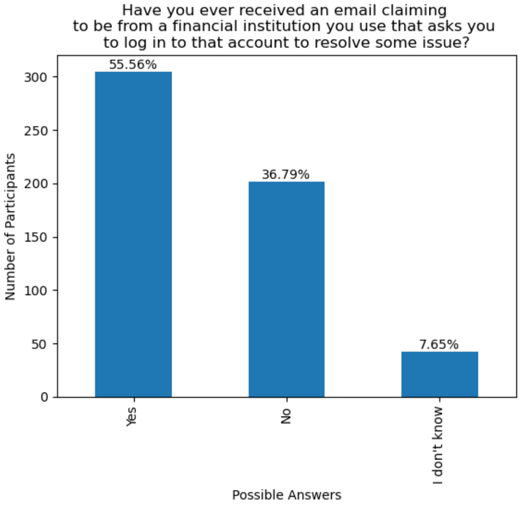


Figure 4.35: Have Participants Ever Received An Email Pretending to Be From a Financial Institution?

In Figure 4.36, most participants (63%) said they were somewhat or extremely likely to be targeted in the future. However, when looking at how each age group answered this question, the 18-24 year old age group was much more likely to say 'extremely unlikely' for whether they thought they would be targeted in the future. The age range 45-54 was slightly more likely to believe that they would be susceptible to being scammed again in the future, with almost no participants age 65 and older saying that they were unlikely to be scammed. See Figure 4.37.

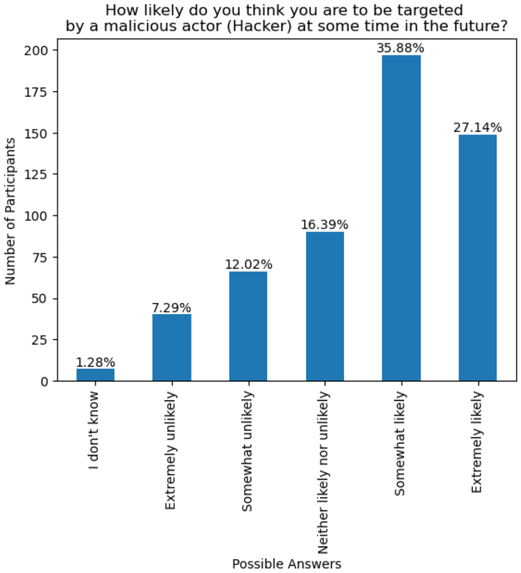
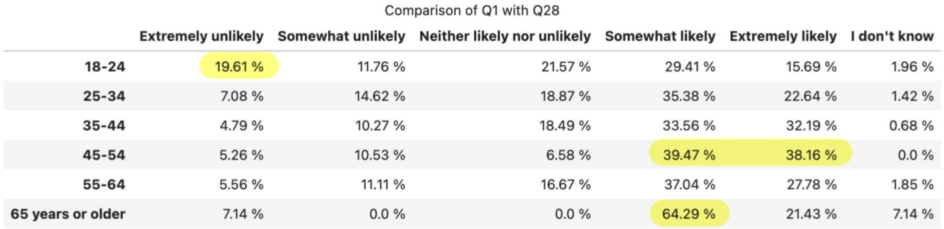


Figure 4.36: Participants Rank of How Likely They are to be Scammed Again on a Five-point scale



Comparison of Q1 with Q28

	Extremely unlikely	Somewhat unlikely	Neither likely nor unlikely	Somewhat likely	Extremely likely	I don't know
18-24	19.61 %	11.76 %	21.57 %	29.41 %	15.69 %	1.96 %
25-34	7.08 %	14.62 %	18.87 %	35.38 %	22.64 %	1.42 %
35-44	4.79 %	10.27 %	18.49 %	33.56 %	32.19 %	0.68 %
45-54	5.26 %	10.53 %	6.58 %	39.47 %	38.16 %	0.0 %
55-64	5.56 %	11.11 %	16.67 %	37.04 %	27.78 %	1.85 %
65 years or older	7.14 %	0.0 %	0.0 %	64.29 %	21.43 %	7.14 %

Figure 4.37: Participants Rank of How Likely They are to be Scammed Again on a Five-point scale, Dissected by Age Range

Chapter 5

Discussion, Conclusions and Future Work

5.1 Overconfidence In Cybersecurity Knowledge

Our group of participants is highly-educated compared to the general population of Maryland. Over 47% of participants have a bachelor's degree and over 29% have a graduate degree. On average in the state of Maryland, only around 23% of residents have a bachelor's degree and less than 20% have a graduate degree. Further, 89.61% of survey participants self-assessed as confident with their computer skills and 74.5% of participants self-assessed as knowledgeable about cybersecurity. These questions were the final two questions asked on the survey, meaning that after participants answered the security questions at least partially incorrectly and stated that almost one in four had been scammed, they still believed that they were very knowledgeable about cybersecurity and had good computer skills.

Even with survey participants being highly educated and self-assessing as knowledgeable about computers and cybersecurity, only 14.03% of participants were able to correctly answer all four of the multiple-choice security questions, and 12.75% of participants did not answer any of the questions correctly. Over 60% of participants scored a two or lower out of four correct answers.

This is concerning because even though these participants have gone through years of schooling to get their degrees and believe that they are knowledgeable on the questioned subjects, there is clearly much more for the average Maryland resident to learn. This shows a need for more computer and cybersecurity training in the state of Maryland, even for people who truly believe that they are prepared. If security training is as common for Maryland residents as it is for the survey participants, where around 62% of participants have had security training within the past year, then clearly something needs to change in the way that we are currently training our residents.

5.2 High Victim Rate of Online Scams

We were surprised by the results of the questions pertaining to on-line scams. Nearly 1 in 4 respondents (23.32%) said they have lost money to an online scam. Additionally, we were surprised by the amounts reported lost. The median loss for those who lost money was $200.00 which was higher than we expected. The average loss was $3,320. This average includes two respondents who reported losing $100,000 each. If we eliminate these 2 responses as outliers, the average loss drops to $1,522. It is important to note that losses in the hundreds of thousands of dollars are not unheard of in online scams.

If we use the numbers above and assume that 23% of Maryland Residents (1.4 Million of Maryland's 6.1 million residents) have lost money to online scams, and that the average loss was $1,522, we arrive, albeit naively, at a loss of $2.1 Billion for Maryland residents. In 2022, the Federal Bureau of Investigation's Internet Crime Report listed reported losses of nearly $218 million for 11,644 victims, an average loss of $18,711. While our survey asks if people have *ever* been scammed and the FBI report is for a single year, we are convinced that this data shows that online scams are under-reported, particularly when the dollar values are low. We believe that further research in this area would be of value to the state of Maryland.

5.3 Password Reuse

There were five possible answers for the survey question 'How do you choose a password for your online accounts?' They follow as:

- **I use passwords that are similar but different for all of my accounts.**
- **I use a unique complex password for my accounts.**
- **I use the same password for most of my accounts.**
- **I use personal information as all or part of my password.**
- **I use the same password for all of my accounts.**

10% of participants use the same password for all of their accounts and over 20% use the same password for most of their accounts. If nearly 1 in 4 participants has been hacked before and over 30% of participants use the same password for most or all of their accounts, 6% of participants have both been hacked and have the same password for most or all of their accounts. The hackers would then be able to easily hack many more of their accounts. While 6% is not a high percentage, that is almost 33 people in this survey alone.

Further, we asked participants how they managed their passwords, and almost 41% of participants said they remembered their passwords. If over 200 people can remember all of their passwords that easily, they must be very similar across accounts. This further emphasizes our finding from before: that many people are not only susceptible to being hacked once, but across all of their accounts if they share the same or a similar password.

We believe that this data about passwords shows how weak people truly secure most of their accounts and how if someone gets scammed once, they are much more likely to be scammed again.

5.4 Ignorance About Data Breaches

Over 45% of people stated that their personal information has been disclosed to unauthorized people. This is almost 250 participants. If we use this data and assume that 45% of Maryland's adult residents have also had personal information disclosed to unauthorized people, that would mean over 2.7 million people have had their personal information breached.

However, we were surprised by this low response rate of 'yes.' We believe that almost everyone's data has been breached before, whether they know it has or not. We believe that the 'no' response rate of almost 38% is extraordinarily high, especially coming from a group of people where almost 1 in 4 have been hacked. Further, we were similarly surprised that over 17% of the participants did not even know whether their personal information had ever been disclosed.

5.5 Significance of the Findings

We believe that our findings show that the state of Maryland needs to invest more in cybersecurity awareness and training for all of its residents. Further, we hope that this effort will be a partnership with the private sector and also become a standard part of the educational process for all students in Maryland.

5.6 Survey Limitations and Recommendations for Future Research

- **Increase Sample Size:** Obtain more respondents to enable more robust statistical analysis of the raw data.
- **Incorporate Interviews:** Conduct interviews with participants to gather more detailed and accurate information about their experiences with cyber scams, including the how, where, and when.
- **Expert Collaboration:** Collaborate with an organization that specializes in survey design and analysis to improve the quality and validity of data collection.
- **Demographic Data Enhancement:** Enhance demographic data collection by including gender information to provide a more comprehensive view of participants.
- **Cross-State Comparison:** Compare the findings of your survey with similar studies conducted in other states to identify regional trends and variations.
- **Reporting Behavior Study:** Investigate whether respondents who have fallen victim to scams reported these incidents to law enforcement. This will help in assessing the underreporting rate of cybercrimes.
- **Phishing Attack Success Rate:** Examine whether respondents who received phishing emails claiming to be from financial institutions were customers of the institution being impersonated. This will shed light on the success rate of phishing attacks.
- **Cybersecurity Awareness Initiatives:** Explore the possibility of establishing a regional or national alliance for cybersecurity awareness and training to address the identified gaps in knowledge and practices.
- **Engage Financial Institutions:** Collaborate with financial institutions that may be interested in the survey results to better understand the financial impact of cybercrimes on individuals.

References

Maryland Department of Planning (2022). Maryland counties socioeconomic characteristics. Accessed April 6, 2023.

United States Census Bureau (2023). Annual county and puerto rico municipio resident population estimates by selected age groups and sex: April 1, 2020 to July 1, 2021 (cc-est2021-agesex). Accessed April 6, 2023.

Appendix A

Survey One-Dimensional Graphs

A.1 Demographic Questions

Age:

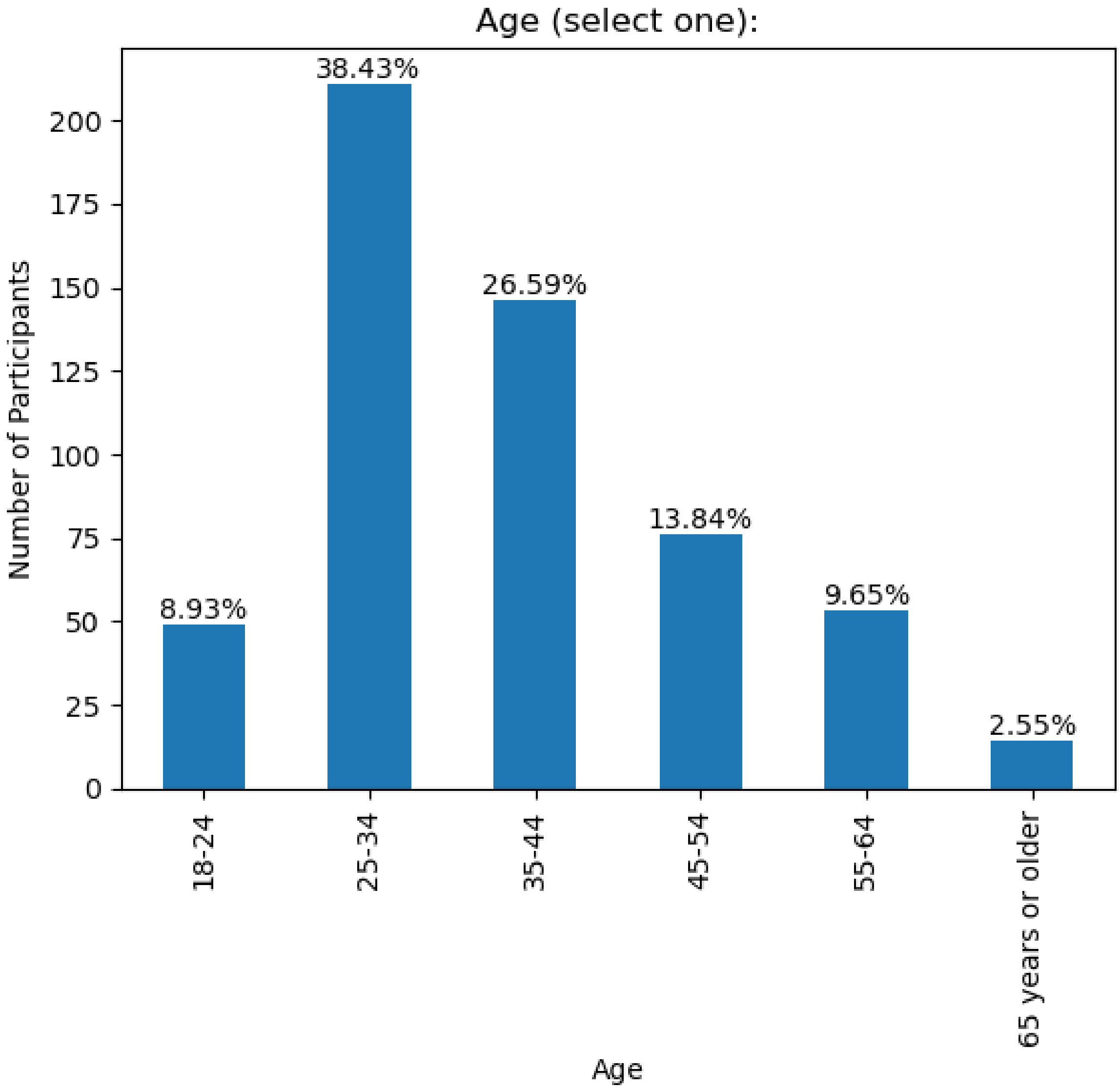


Figure A.1: Age Distribution

Primary Residence County:

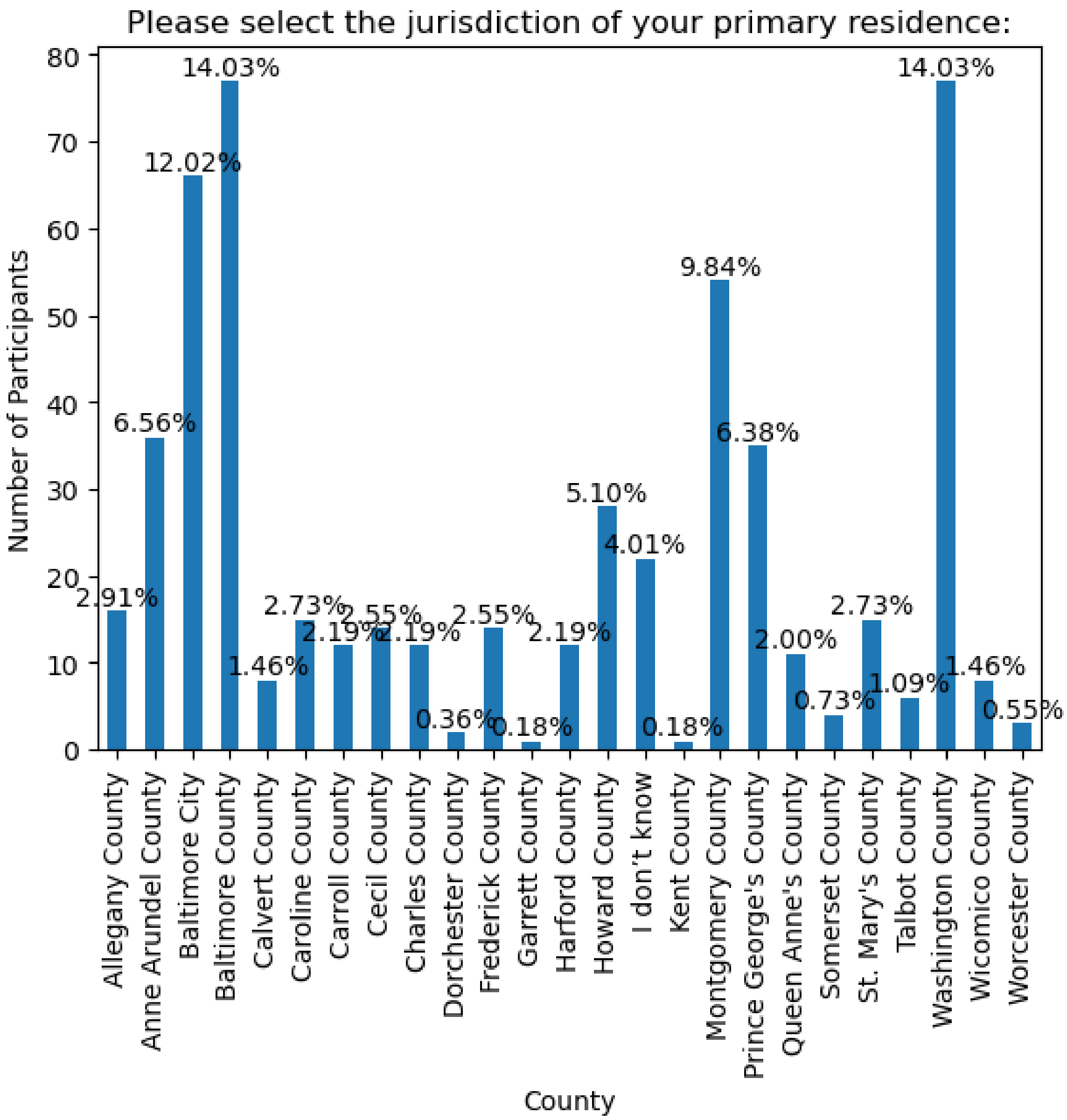


Figure A.2: County of Primary Residence

Primary Residence Region:

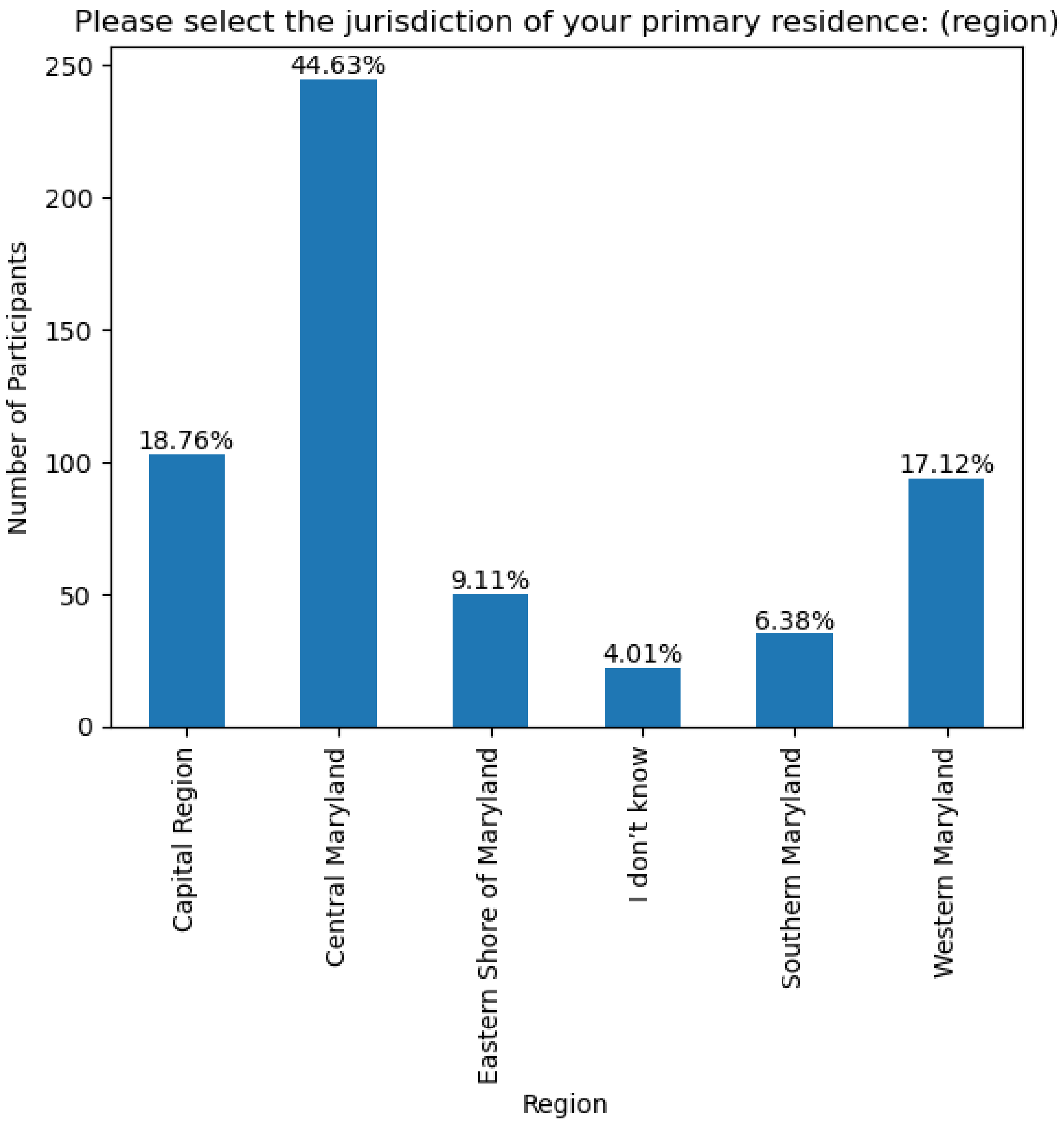


Figure A.3: Region of Primary Residence

Education Level:

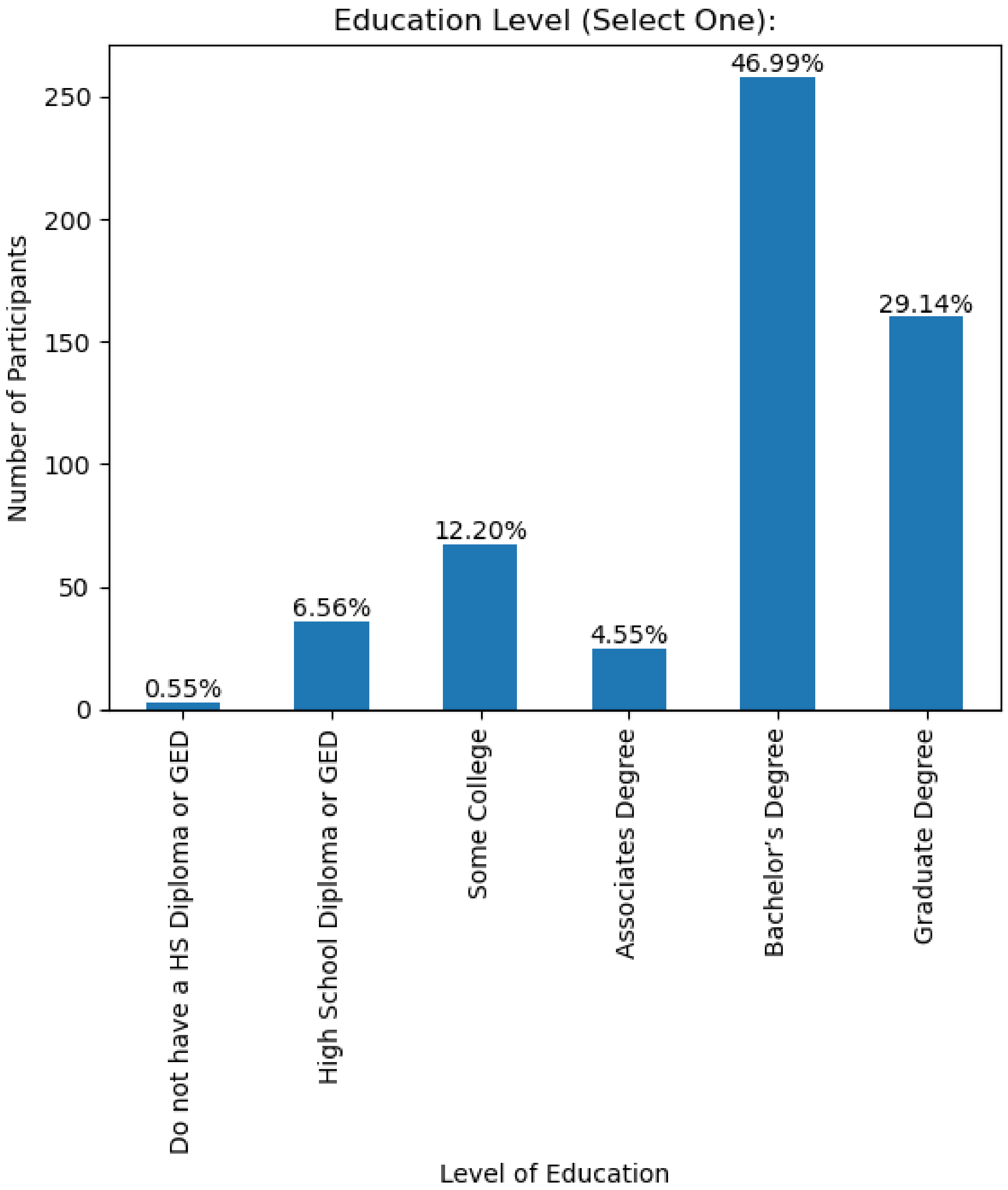


Figure A.4: Education Level Distribution

Year of Birth:

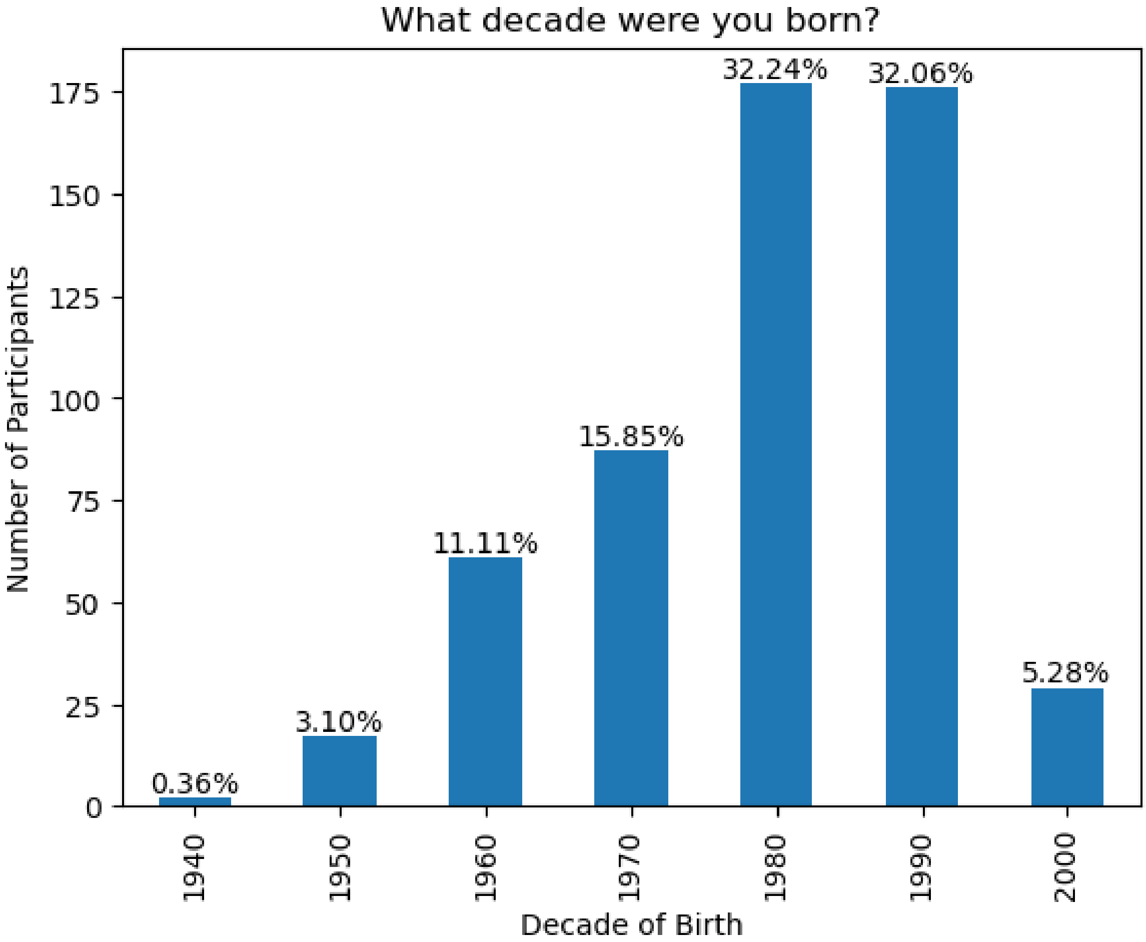


Figure A.5: Year of Birth Distribution

A.2 Backup Behavior Questions

Backup Methods:

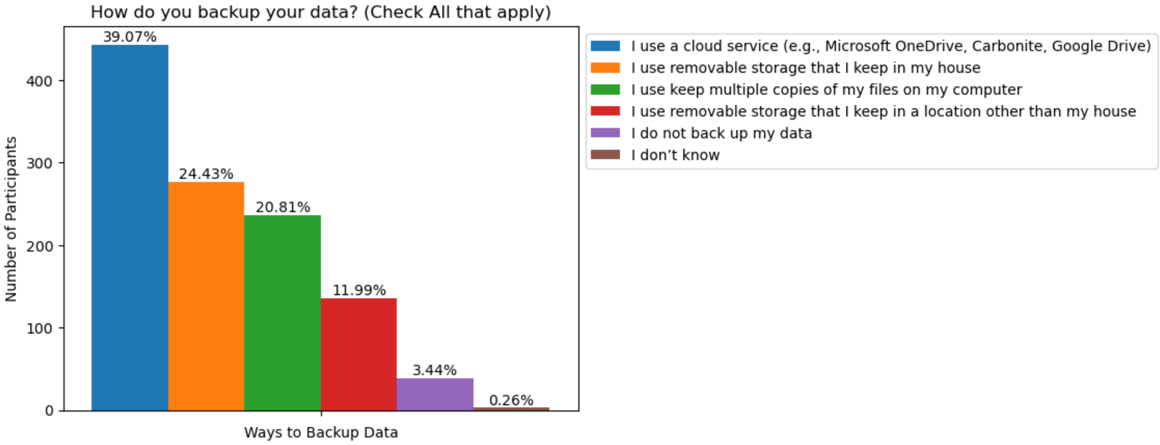


Figure A.6: Backup Methods

Backup Frequency:

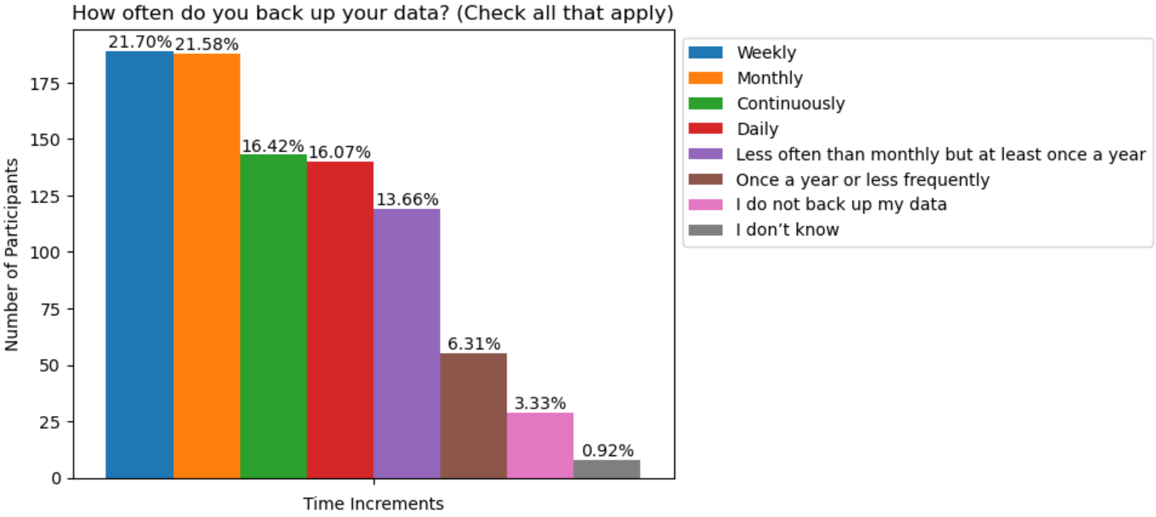


Figure A.7: Backup Frequency

Last Backup Validation:

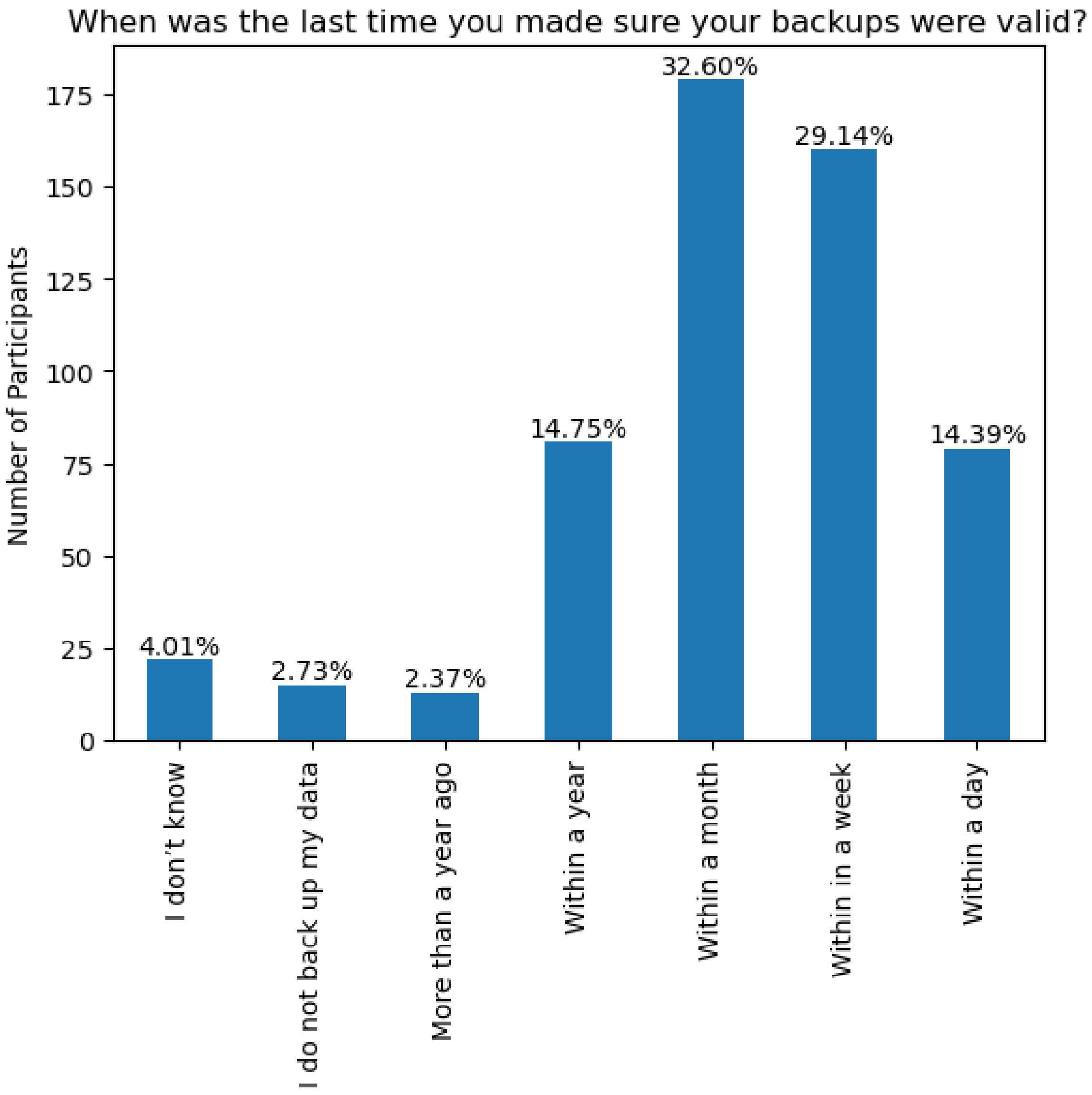


Figure A.8: Last Backup Validation

A.3 Security Awareness Questions

Social Engineering Definition:

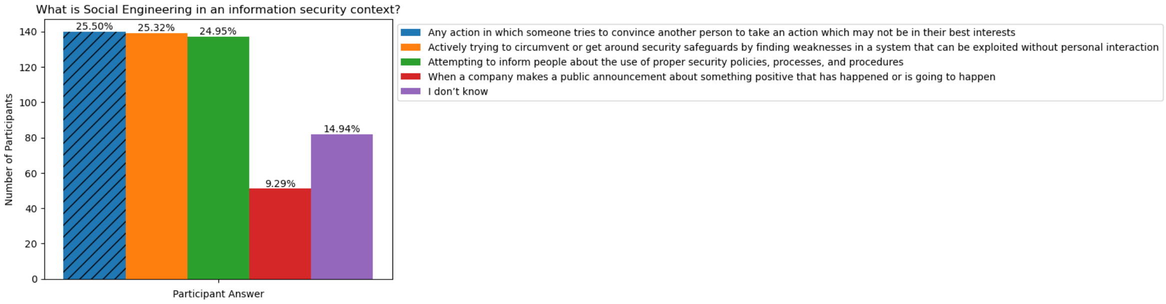


Figure A.9: Social Engineering Definition

Spear Phishing Definition:

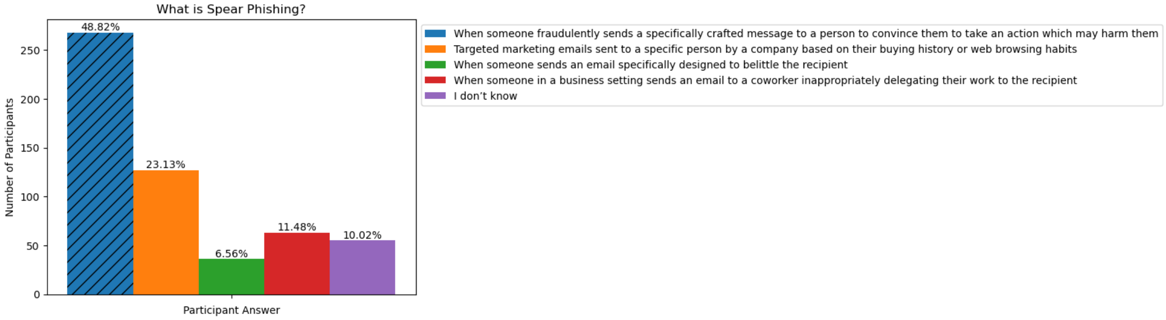


Figure A.10: What is Spear Phishing?

Phishing Definition:

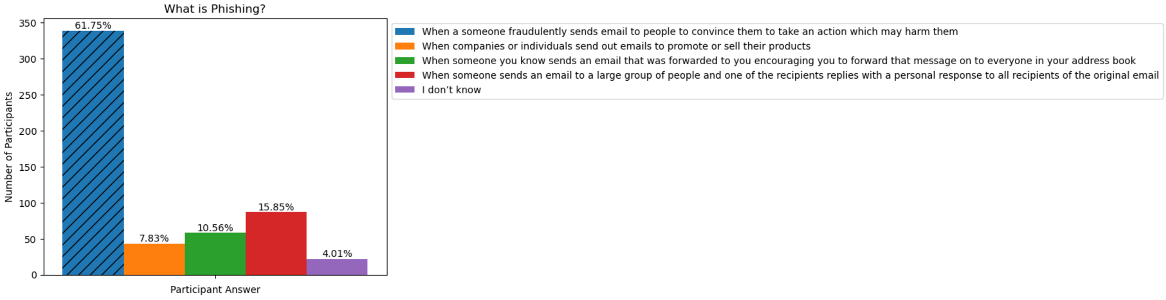


Figure A.11: What is Phishing?

Multifactor Authentication Definition:

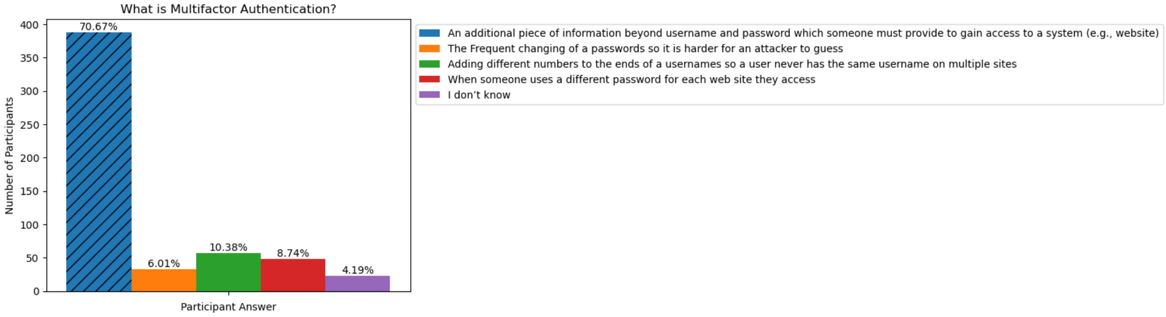


Figure A.12: What is Multifactor Authentication

A.4 Security Hygiene Questions

Where do you use multifactor authentication?

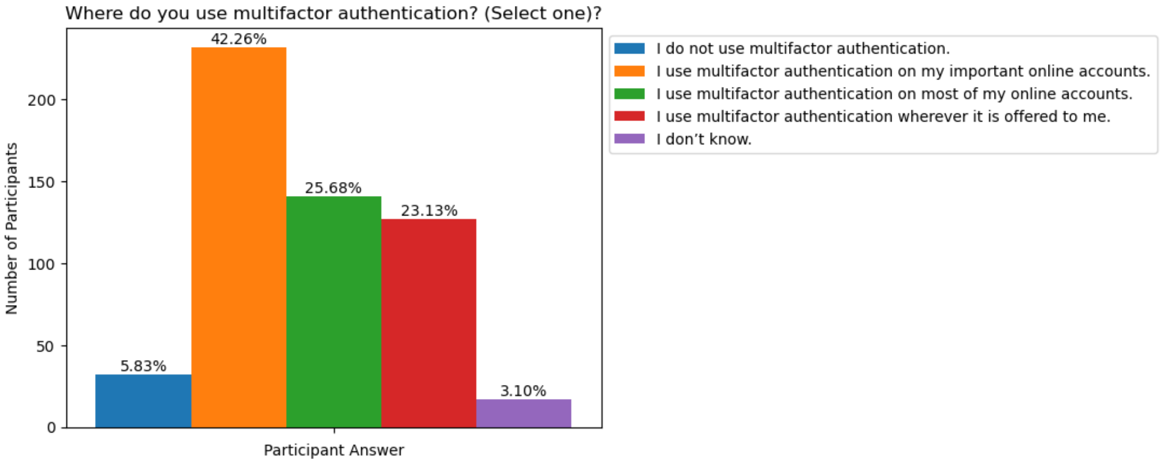


Figure A.13: Where do you use multifactor authentication?

What form of multifactor authentication do you use?

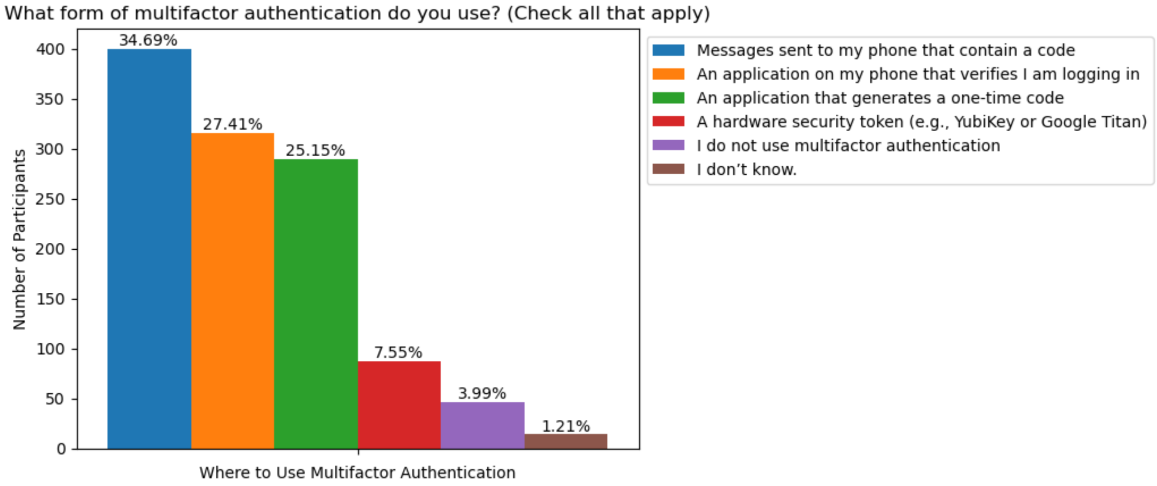
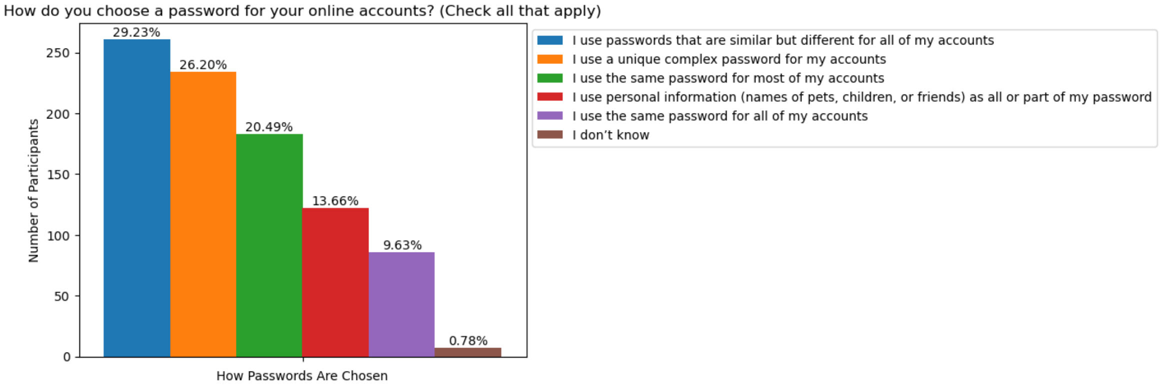


Figure A.14: What form of multifactor authentication do you use?

How do you choose a password for your online accounts?



centering

Figure A.15: How do you choose a password for your online accounts?

How do you manage the passwords for your online accounts?

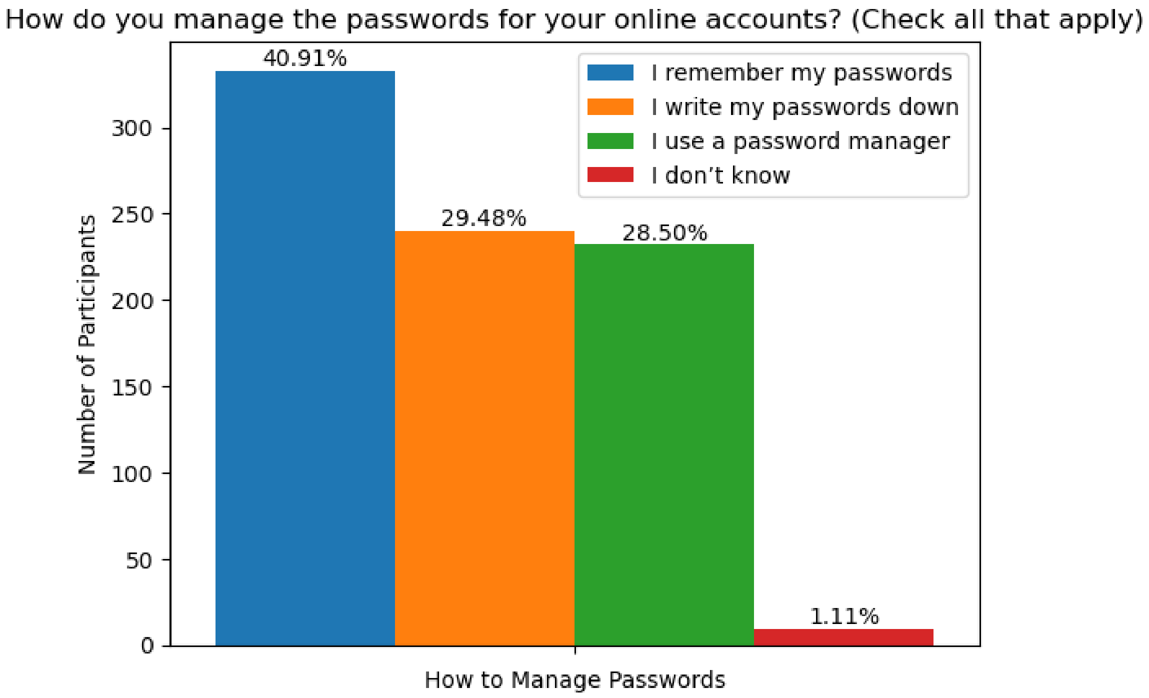


Figure A.16: How do you manage the passwords for your online accounts?

When have you ever received security awareness training at your place of employment or through other means such as a community organization or an advocacy group?

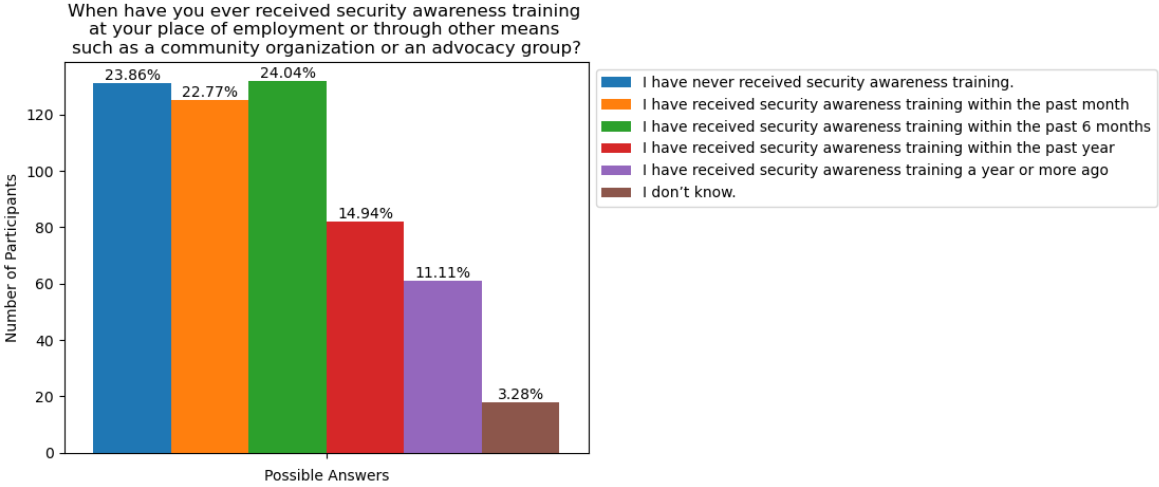


Figure A.17: When have you ever received security awareness training at your place of employment or through other means such as a community organization or an advocacy group?

A.5 History Questions

Have you ever been the victim of ransomware?

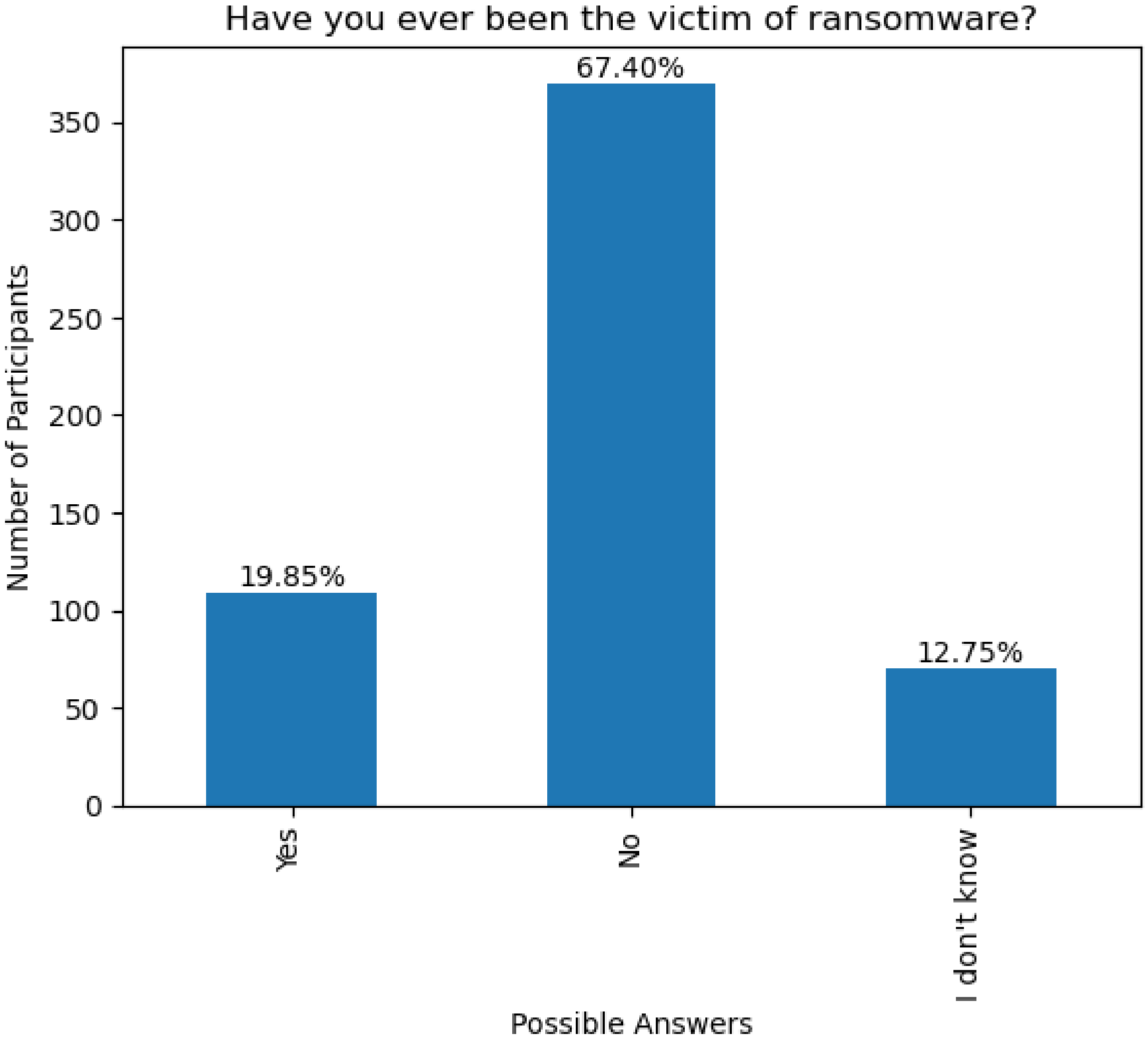


Figure A.18: Have you ever been the victim of ransomware?

To your knowledge, has your personal information been disclosed to unauthorized people, e.g., via a data breach?

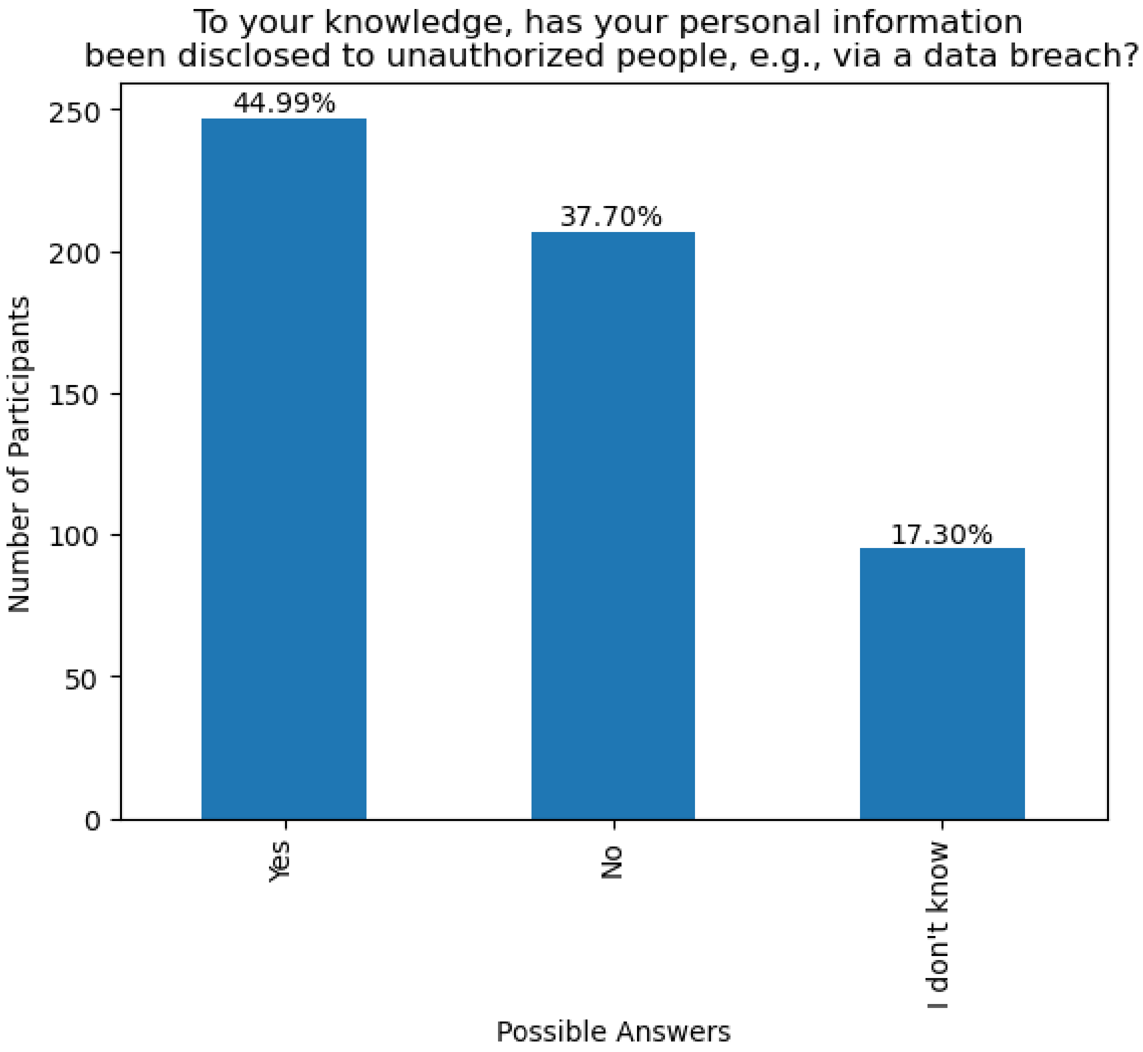


Figure A.19: To your knowledge, has your personal information been disclosed to unauthorized people, e.g., via a data breach?

Have you ever been the victim of an online scam where you lost any amount of money?

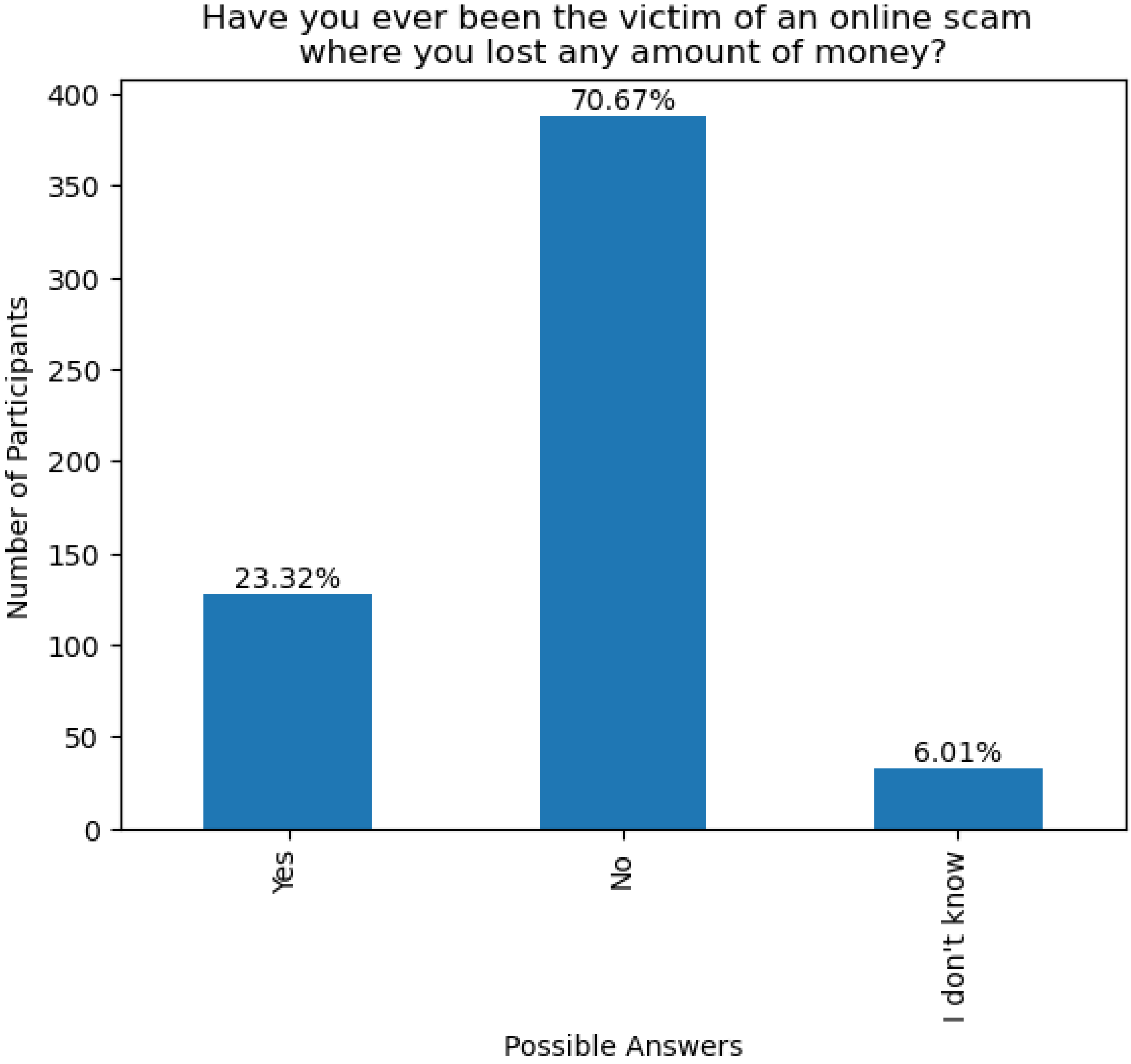


Figure A.20: Have you ever been the victim of an online scam where you lost any amount of money?

Loss Due to Scam Victimization

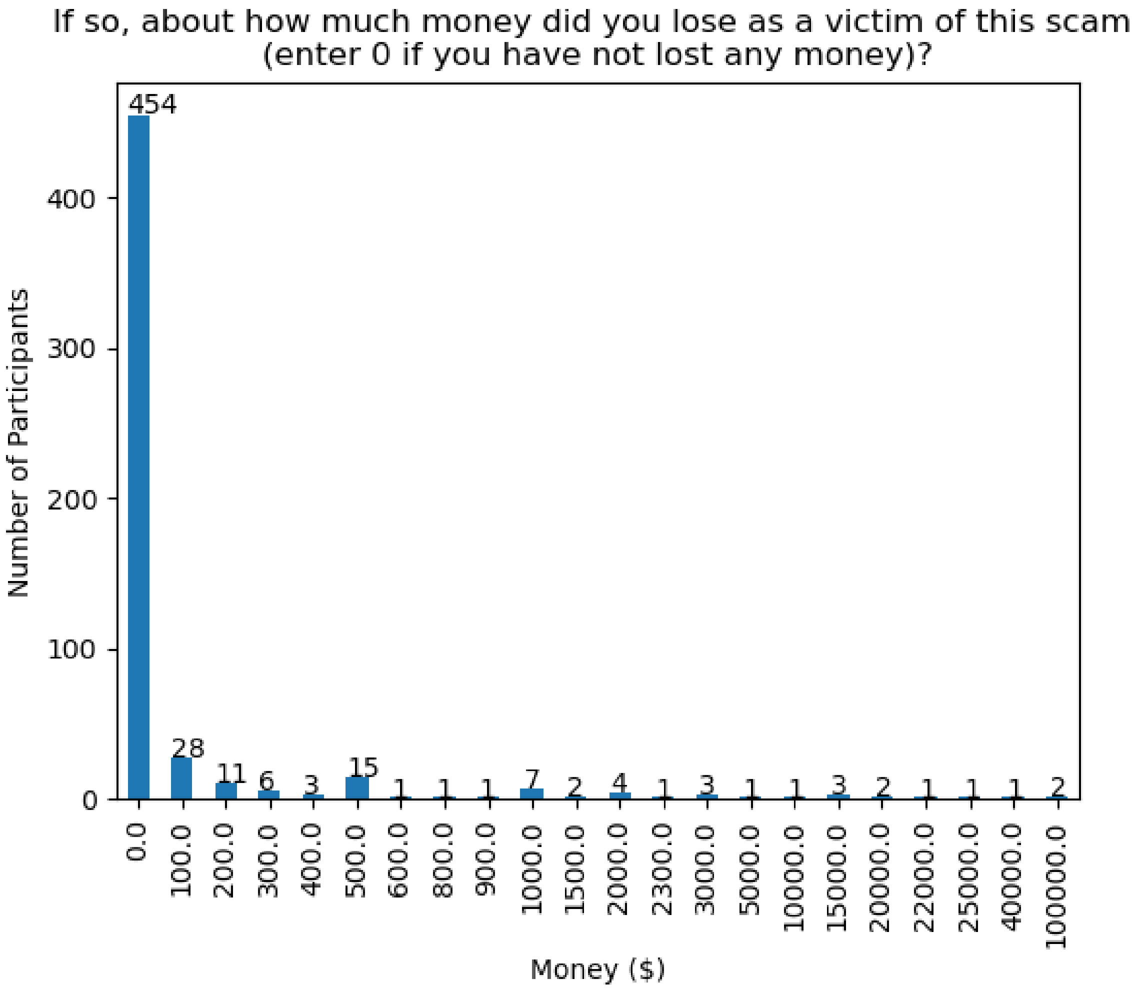


Figure A.21: If so, about how much money did you lose as a victim of this scam (enter 0 if you have not lost any money)? - INCLUDING the answer 0

Loss Due to Scam Victimization - without 0

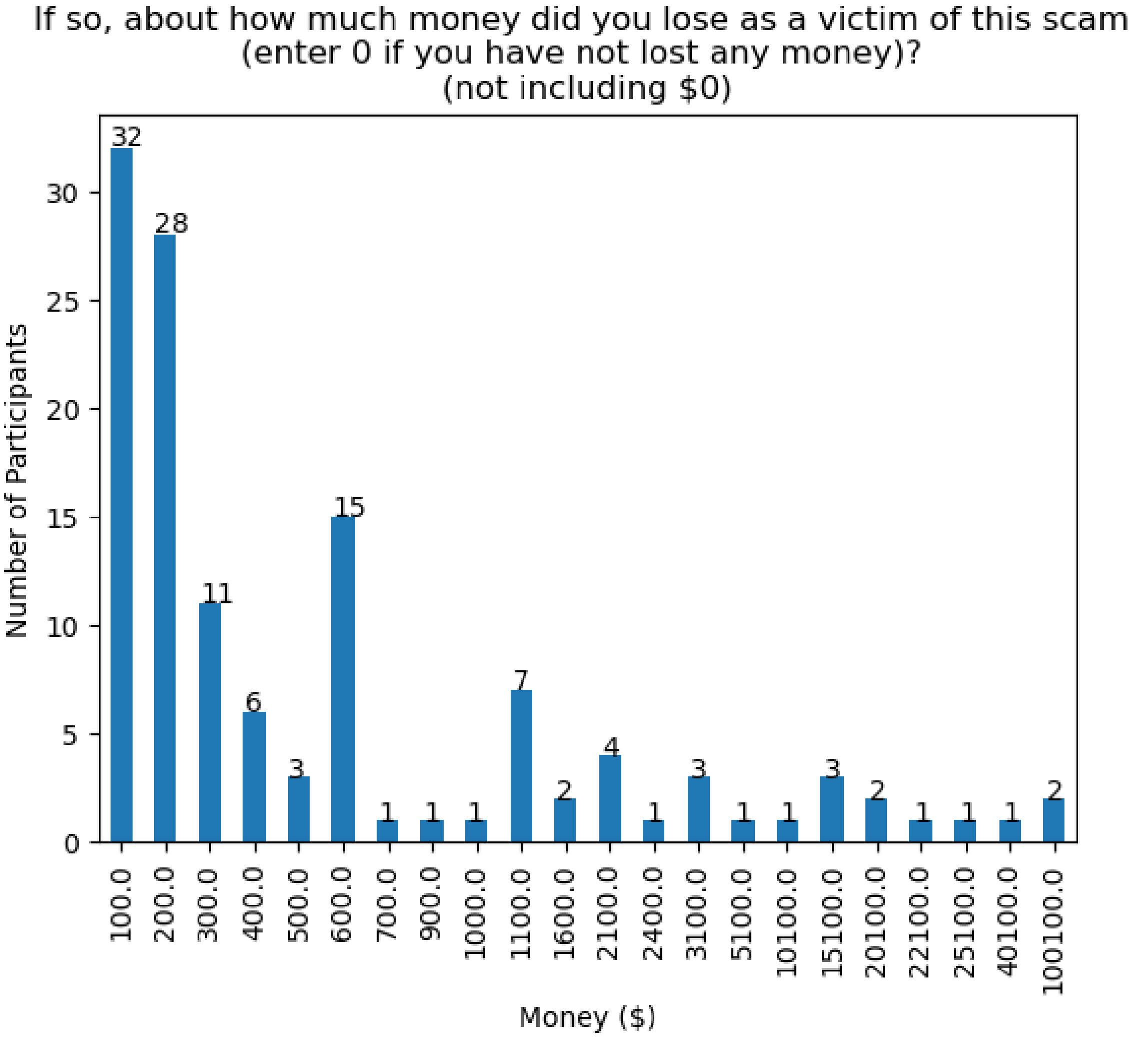


Figure A.22: If so, about how much money did you lose as a victim of this scam (enter 0 if you have not lost any money)? - NOT INCLUDING the answer 0

Phone Scam Experience

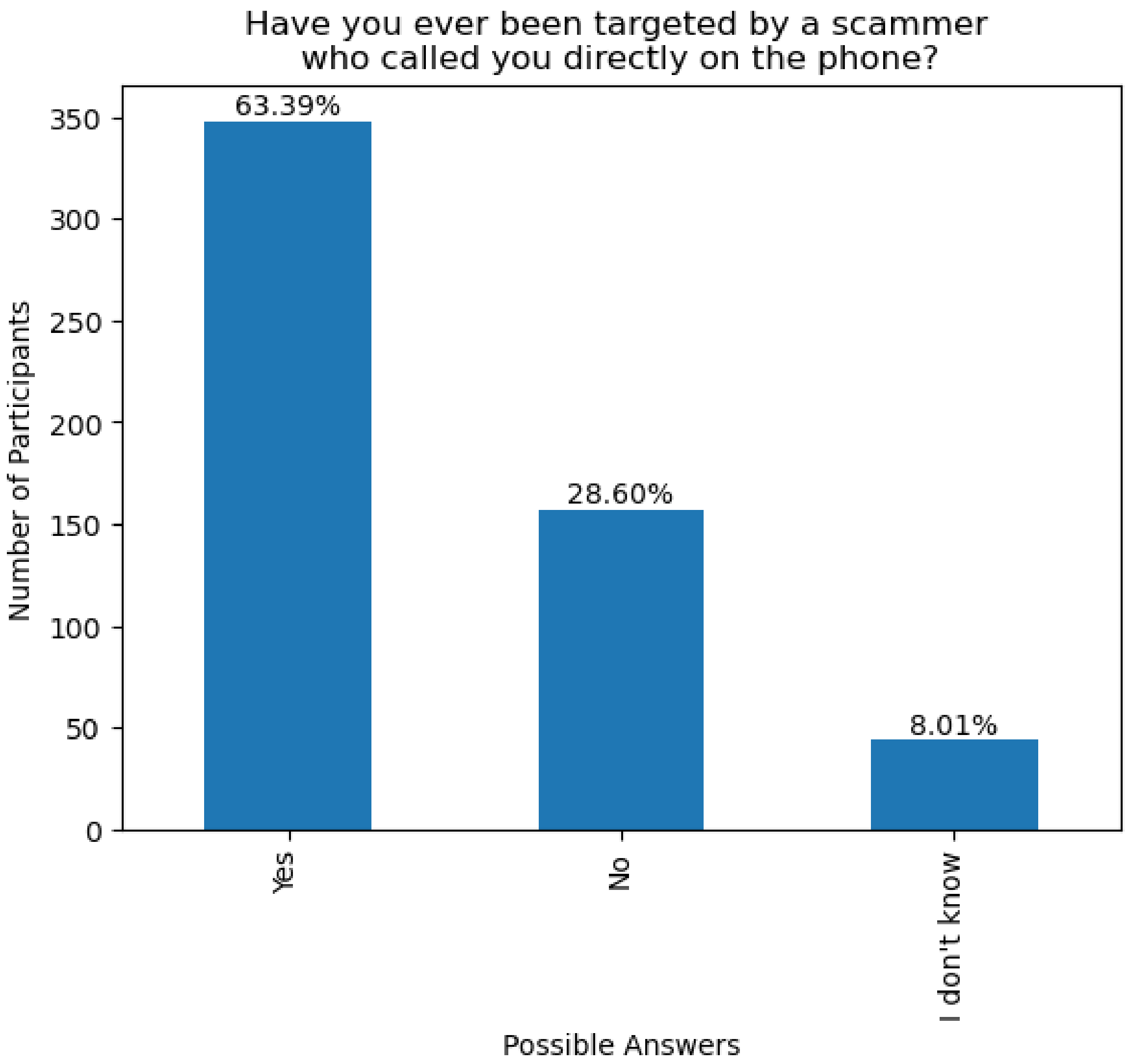


Figure A.23: Have you ever been targeted by a scammer who called you directly on the phone?

Online Account Takeover

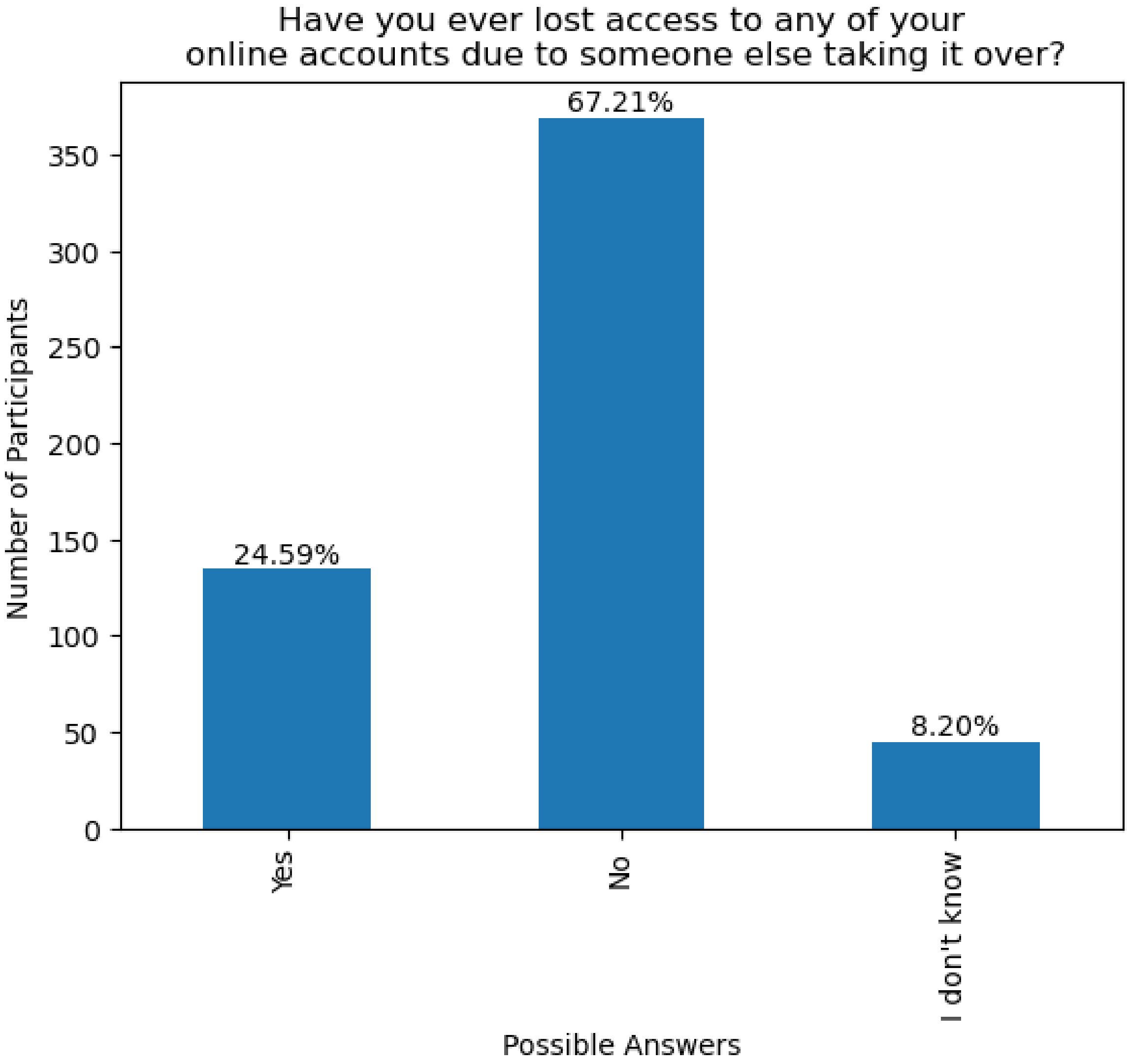


Figure A.24: Have you ever lost access to any of your online accounts due to someone else taking it over?

Phishing Emails from Financial Institutions

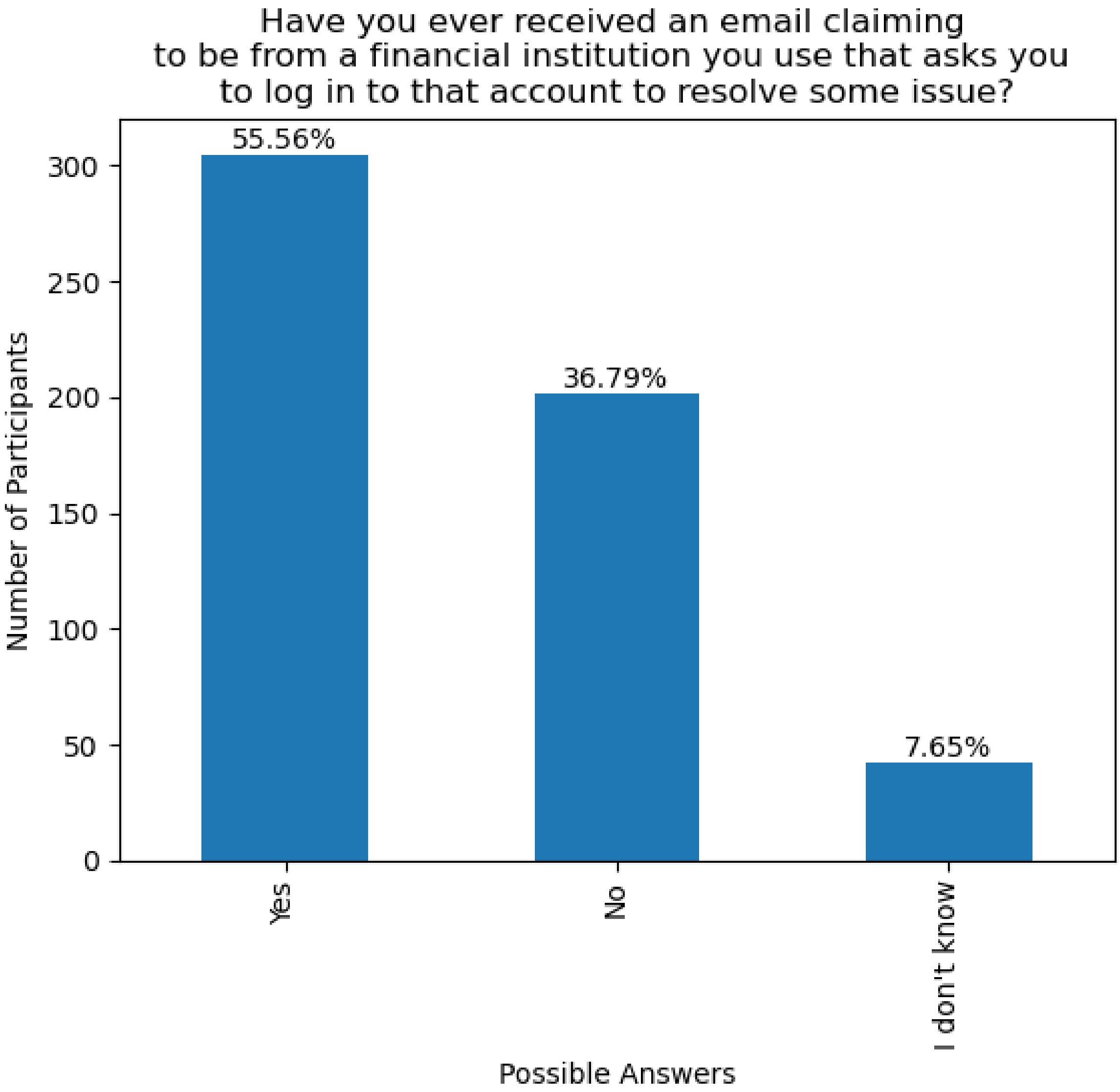


Figure A.25: Have you ever received an email claiming to be from a financial institution you use that asks you to log in to that account to resolve some issue?

Likelihood of Future Hacking

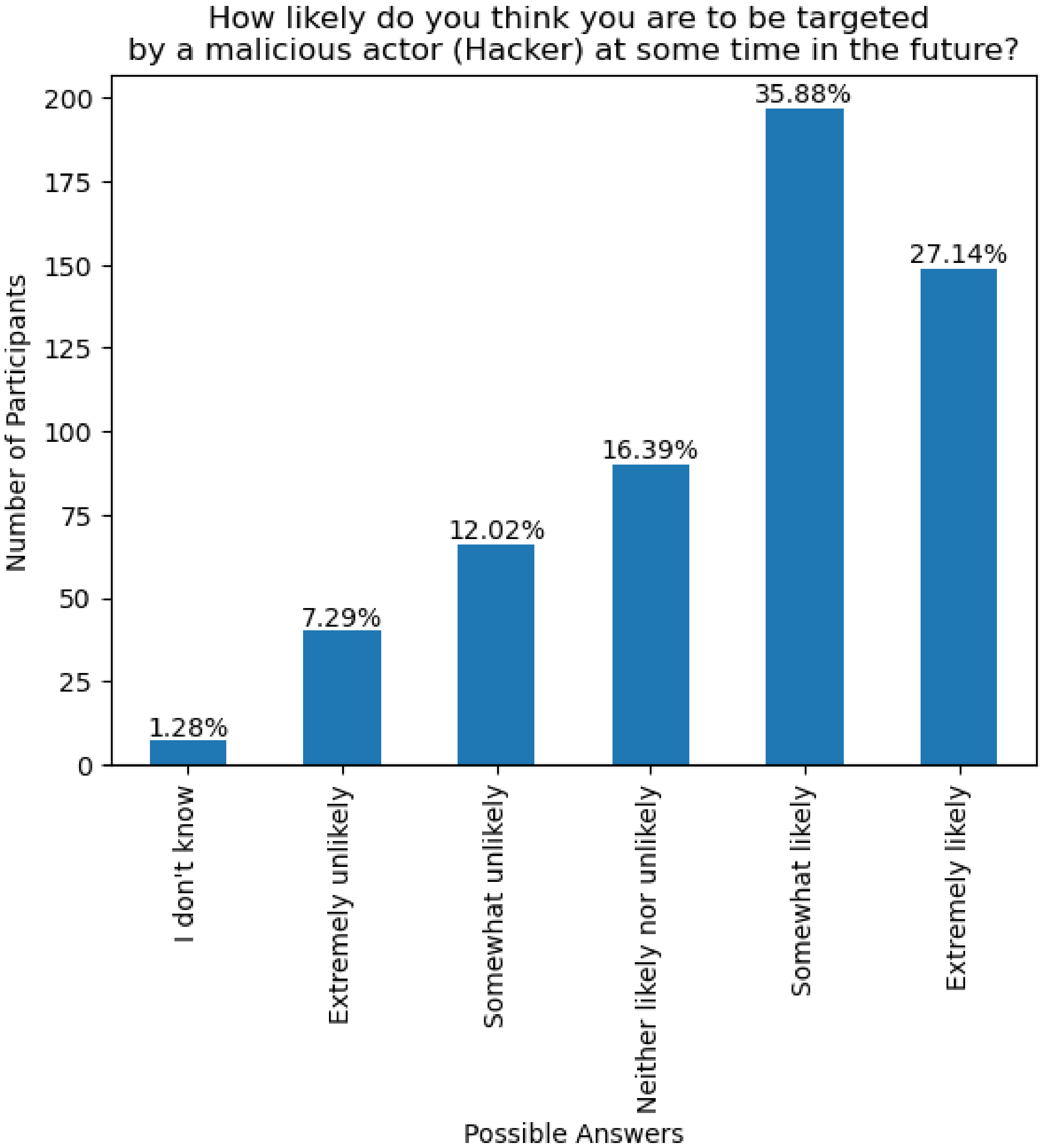


Figure A.26: How likely do you think you are to be targeted by a malicious actor (Hacker) at some time in the future? (5 point scale + I don't know)

A.6 Final Questions

Confidence in Computer Skills

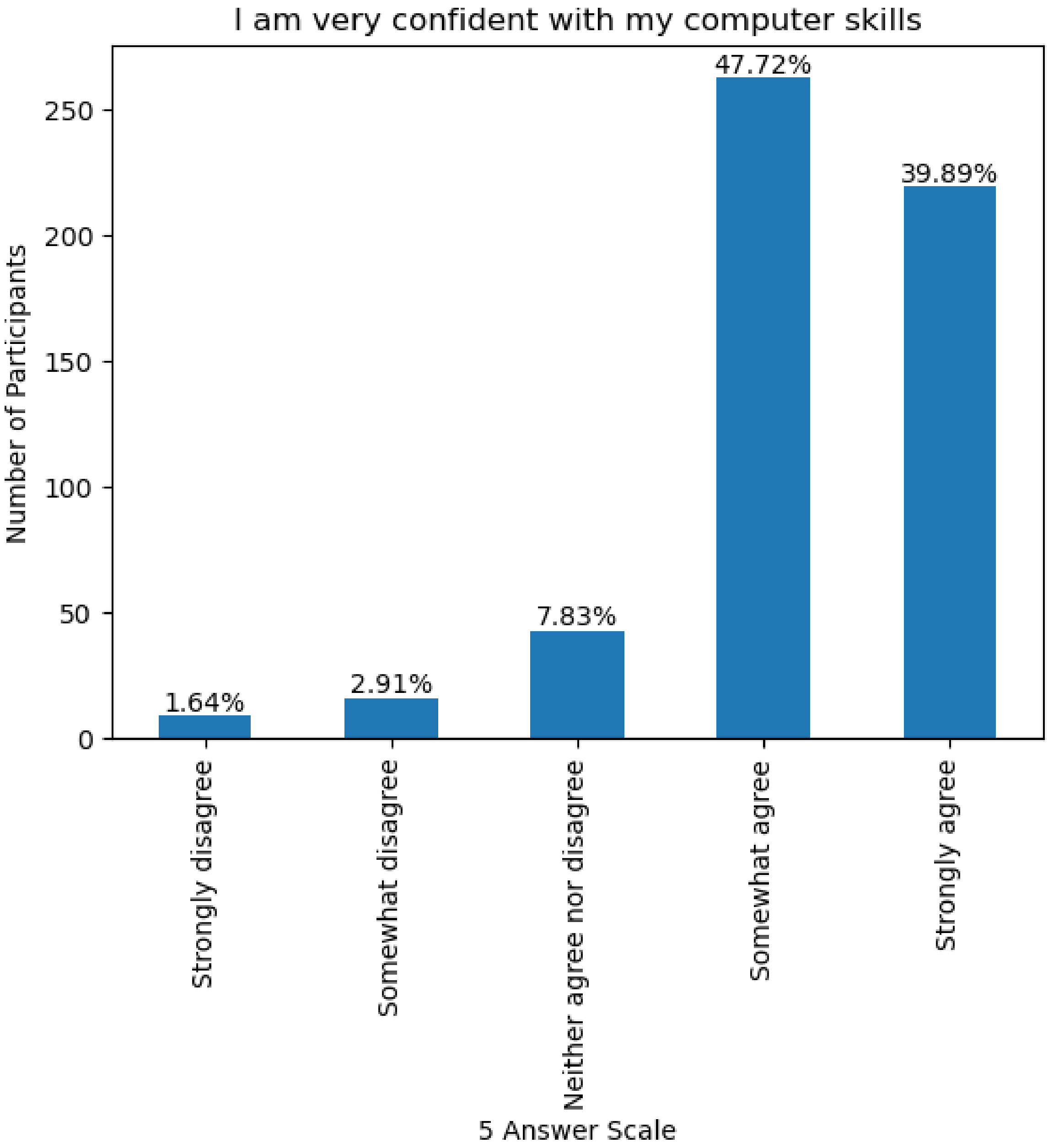


Figure A.27: I am very confident with my computer skills. (5 point Agree/Disagree scale)

Confidence in Cybersecurity Knowledge

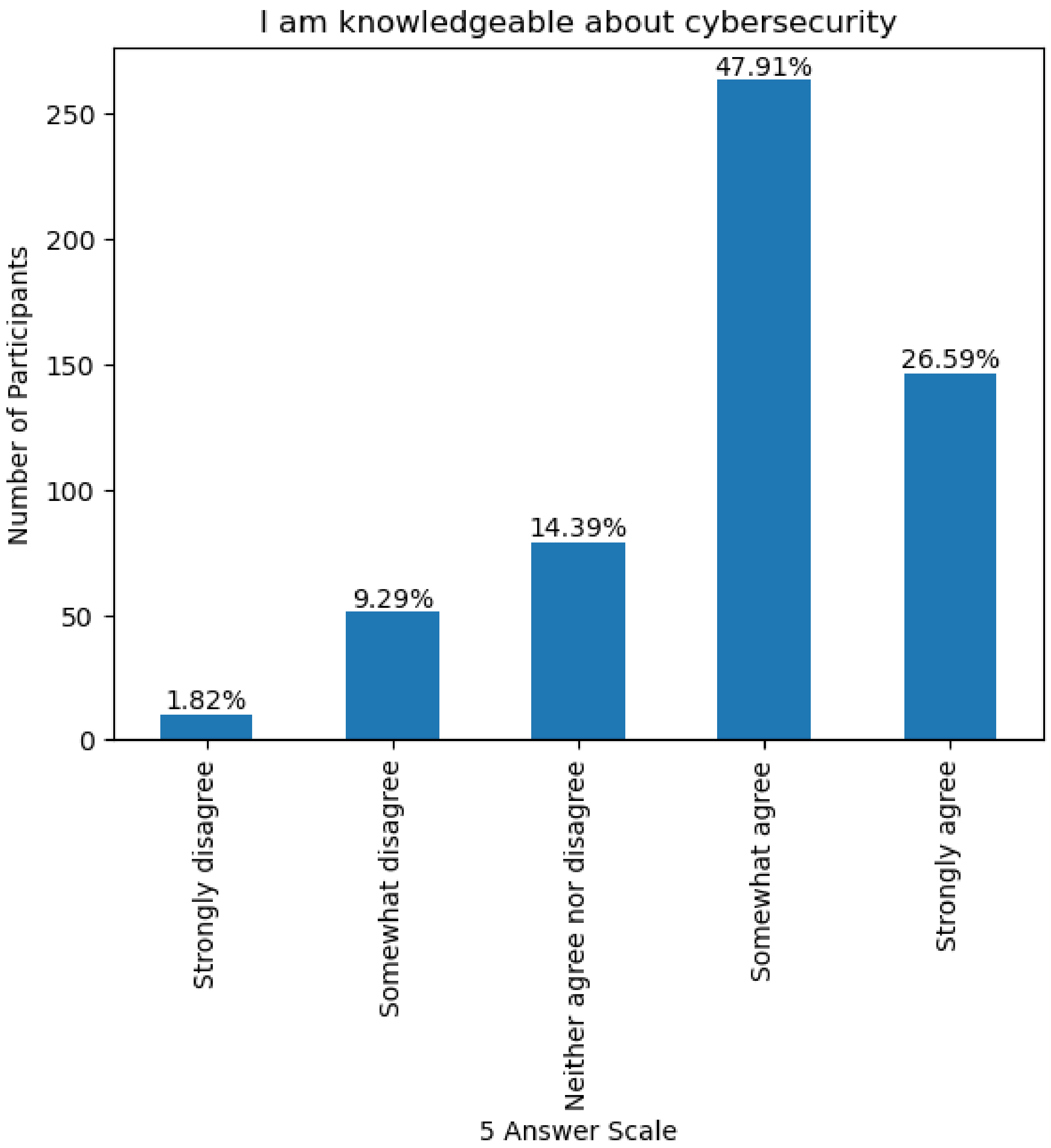


Figure A.28: I am knowledgeable about cybersecurity. (5 point Agree/Disagree scale)

Appendix B

Maryland 2020 Census Data Compared to Survey Data

B.1 Age

Age Group for All Maryland Residents

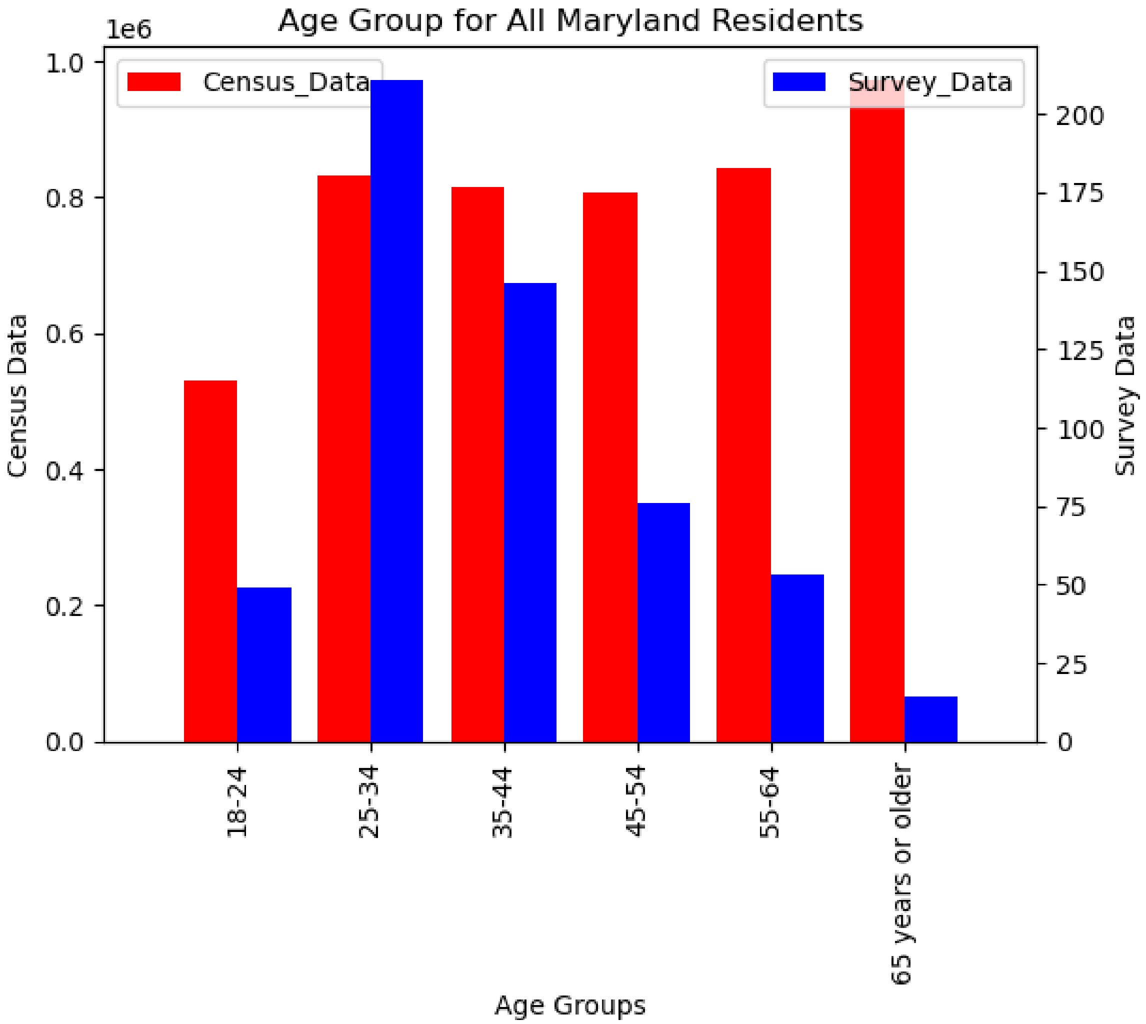


Figure B.1: Survey vs Census: Maryland Residents in State by Age Range

Jurisdiction of Primary Residence for All Maryland Residents

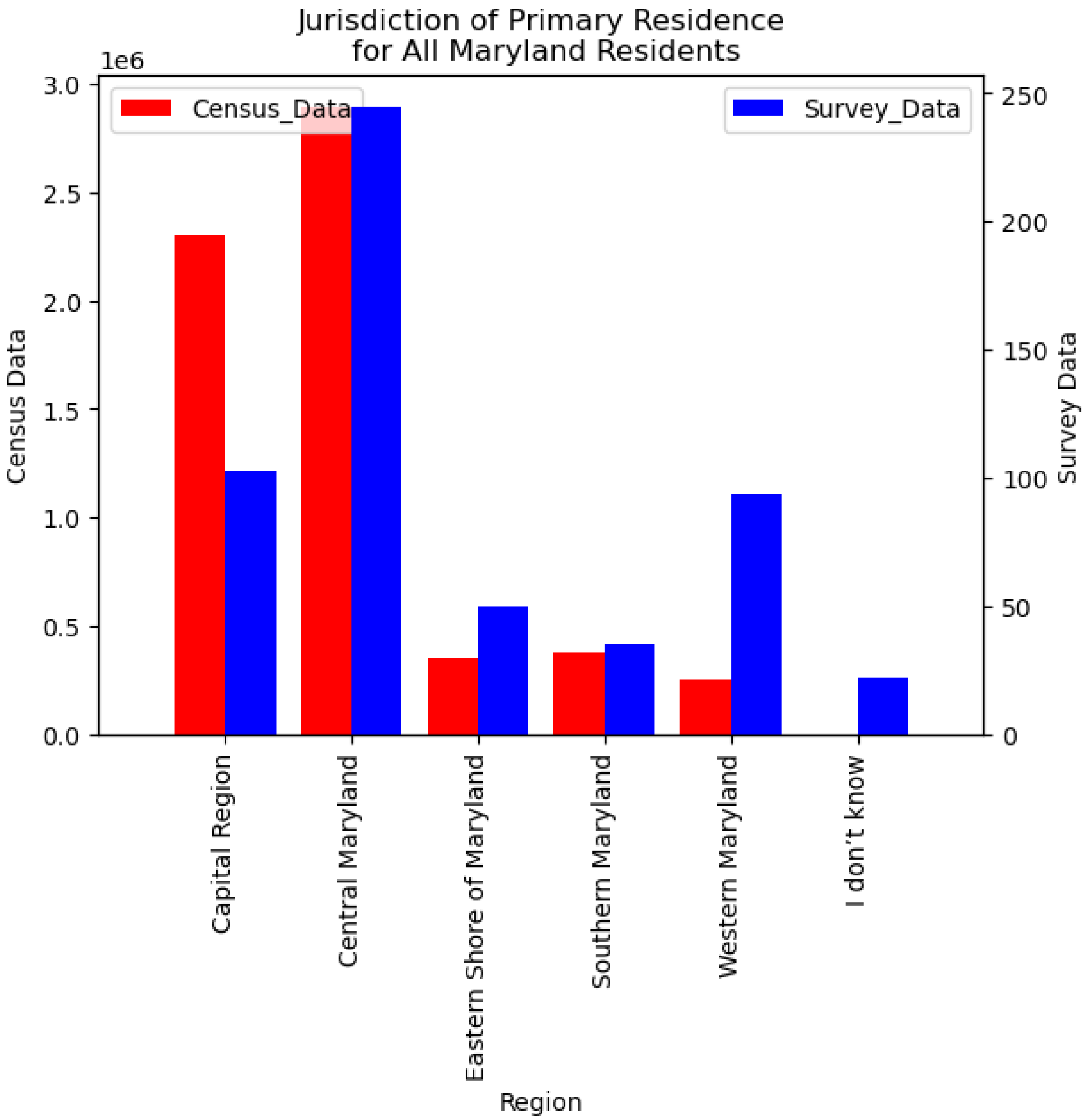


Figure B.2: Survey vs Census: Jurisdiction of Primary Residence for All Maryland Residents

Age 18-24 Per Maryland Region

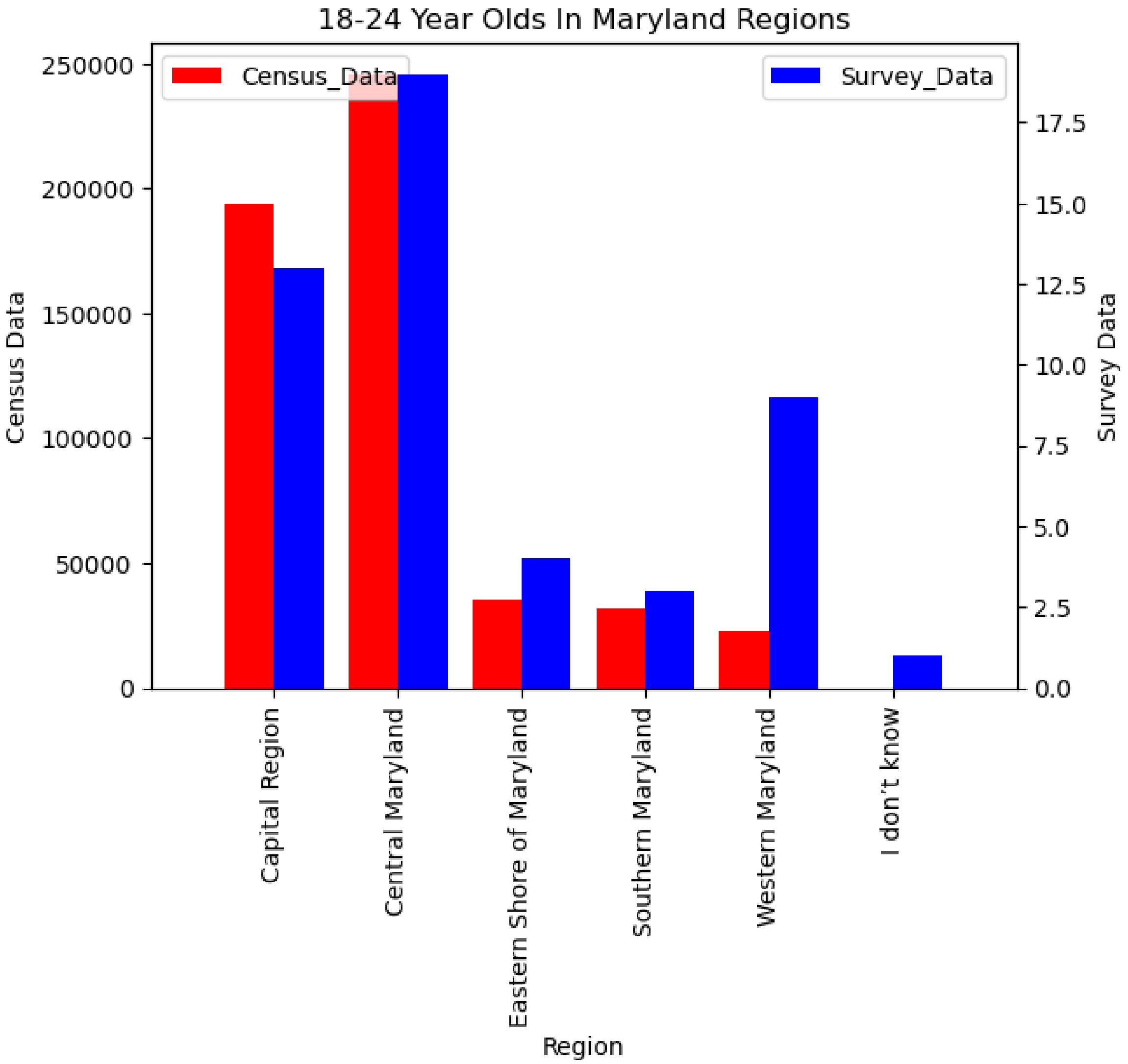


Figure B.3: Survey vs Census: Maryland Residents Age 18-24 by Region

Age 25-34 Per Maryland Region

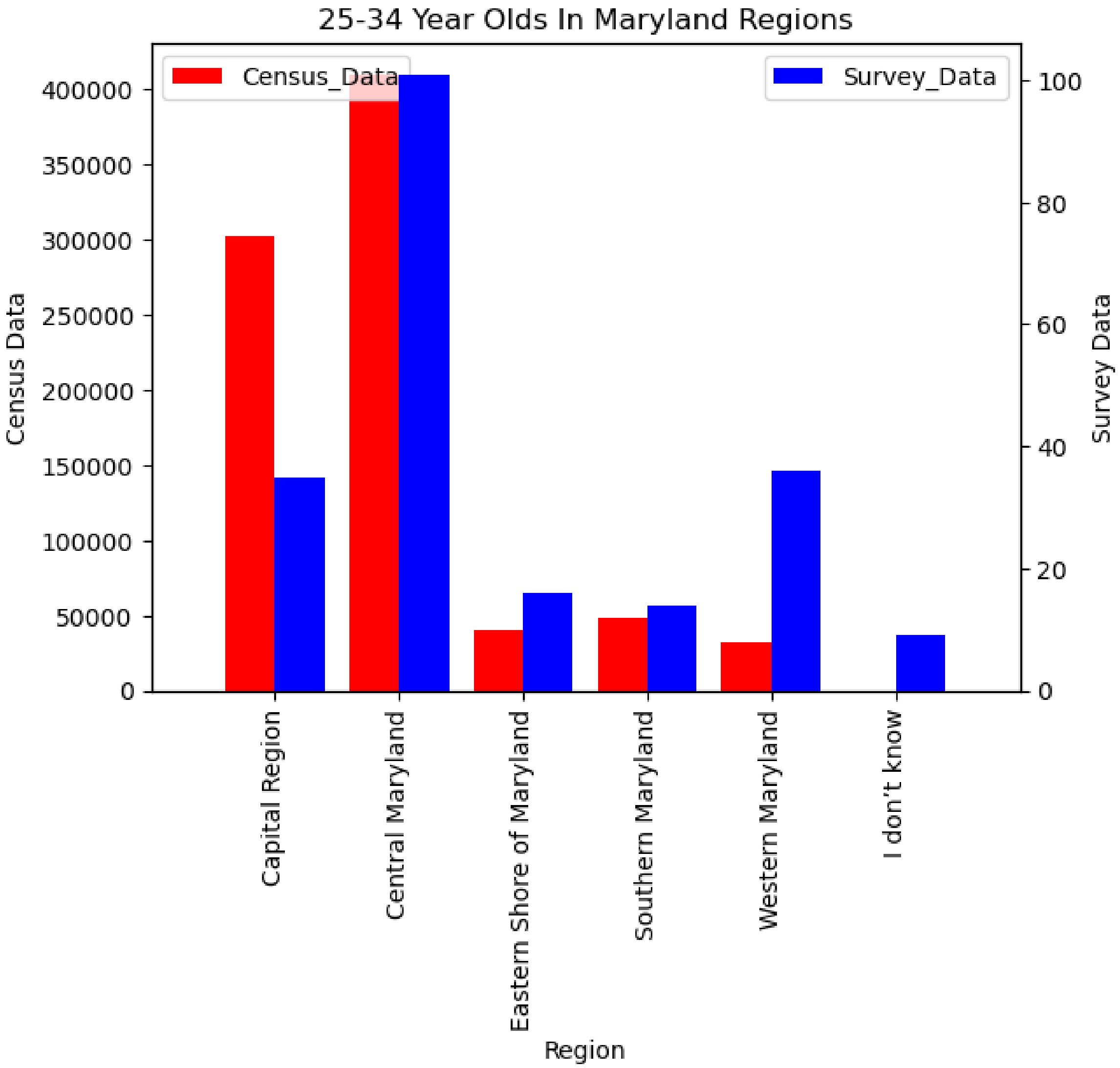


Figure B.4: Survey vs Census: Maryland Residents Age 25-34 by Region

Age 35-44 Per Maryland Region

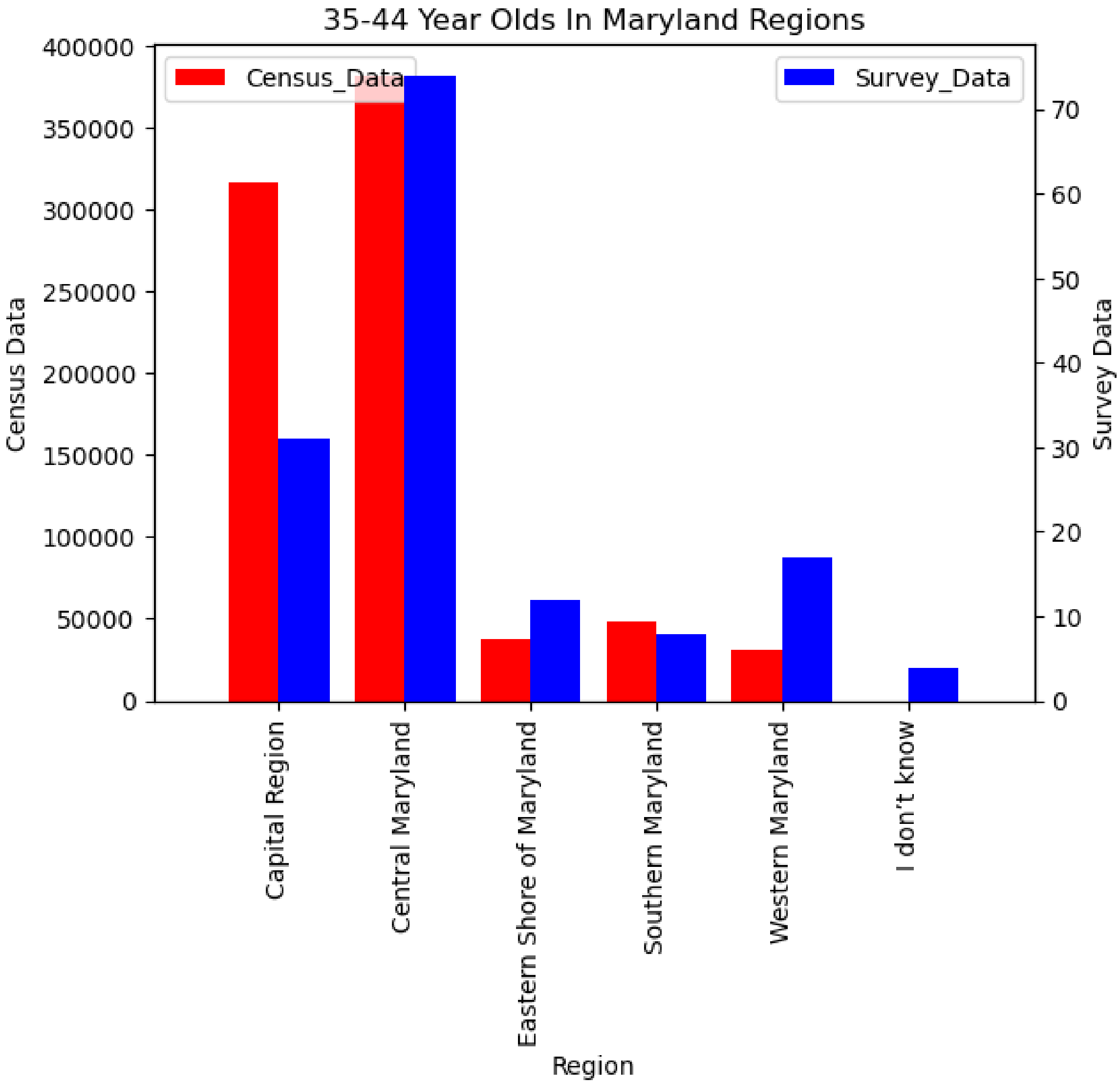


Figure B.5: Survey vs Census: Maryland Residents Age 35-44 by Region

Age 45-54 Per Maryland Region

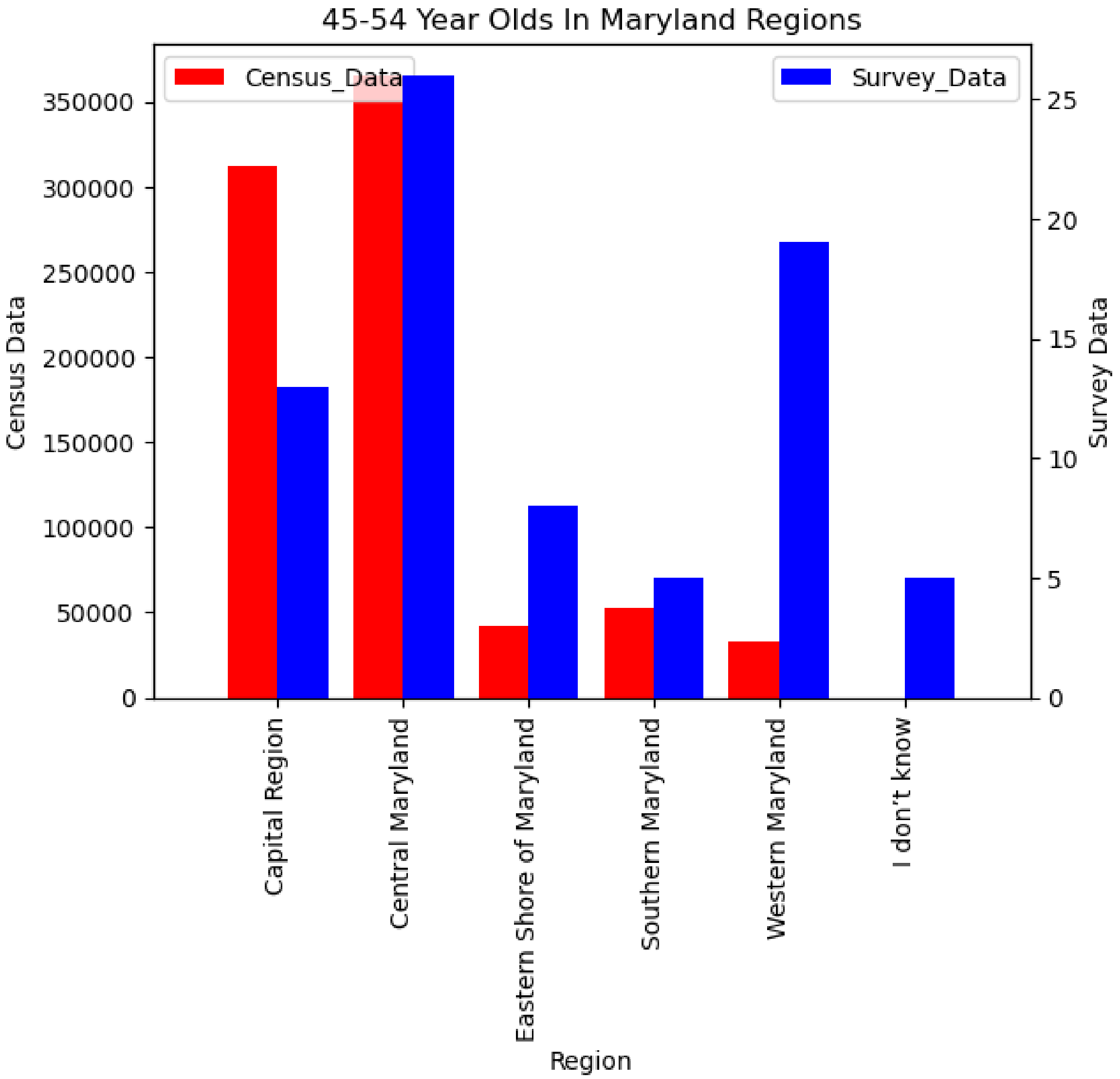


Figure B.6: Survey vs Census: Maryland Residents Age 45-54 by Region

Age 55-64 Per Maryland Region

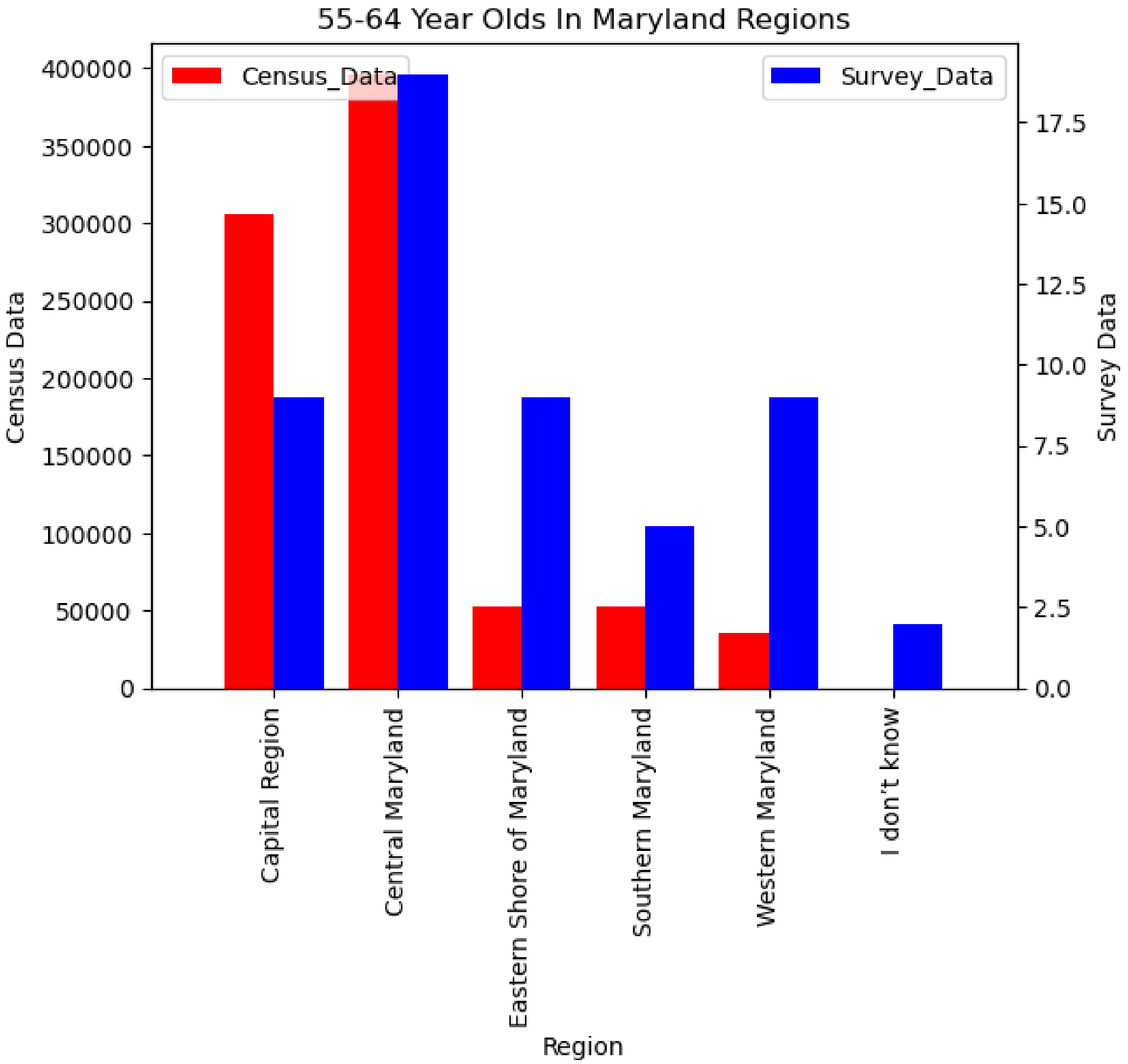


Figure B.7: Survey vs Census: Maryland Residents Age 55-64 by Region

Age 65+ Per Maryland Region

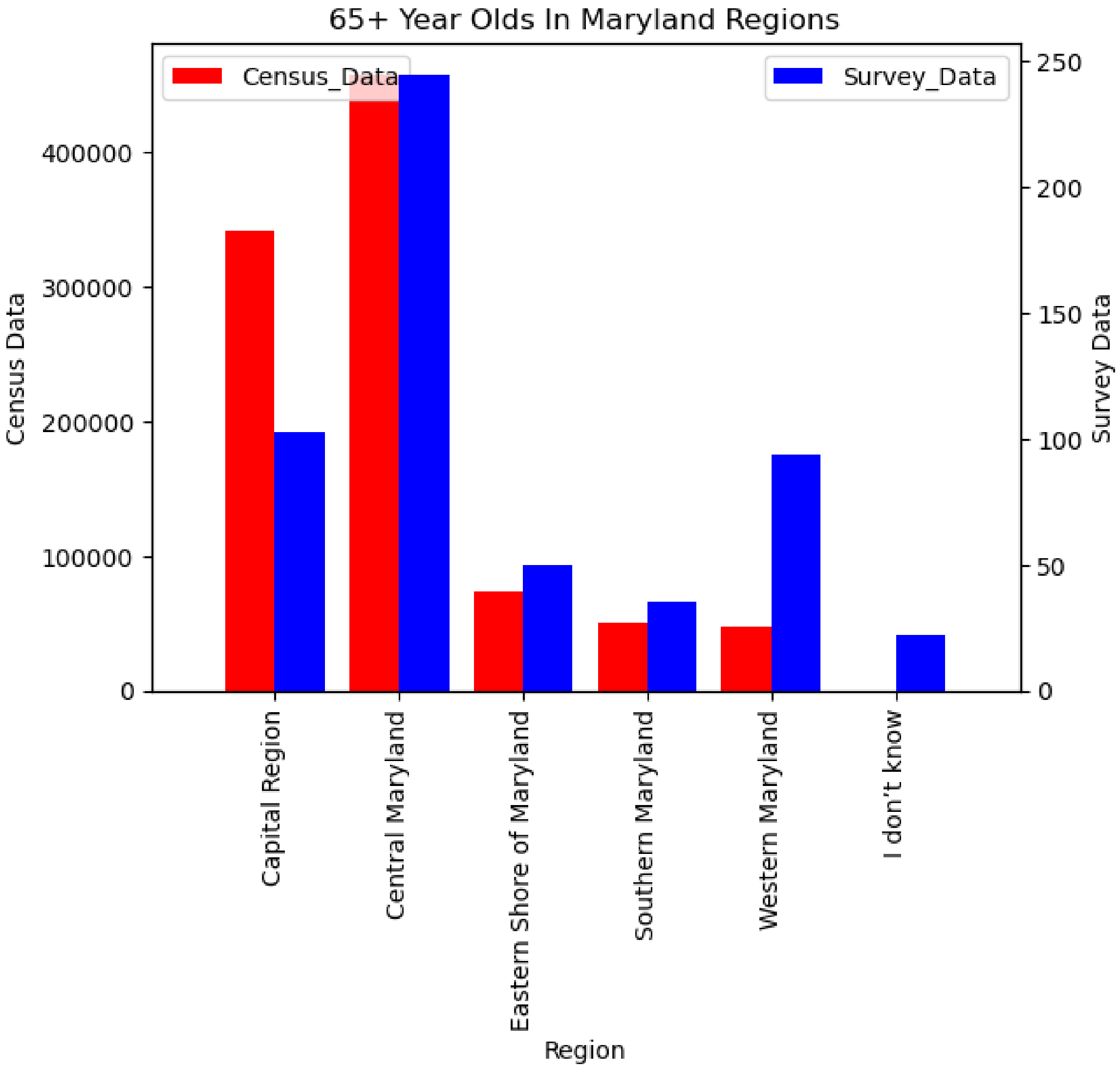


Figure B.8: Survey vs Census: Maryland Residents Age 65+ by Region

Total Age Per Capital Region

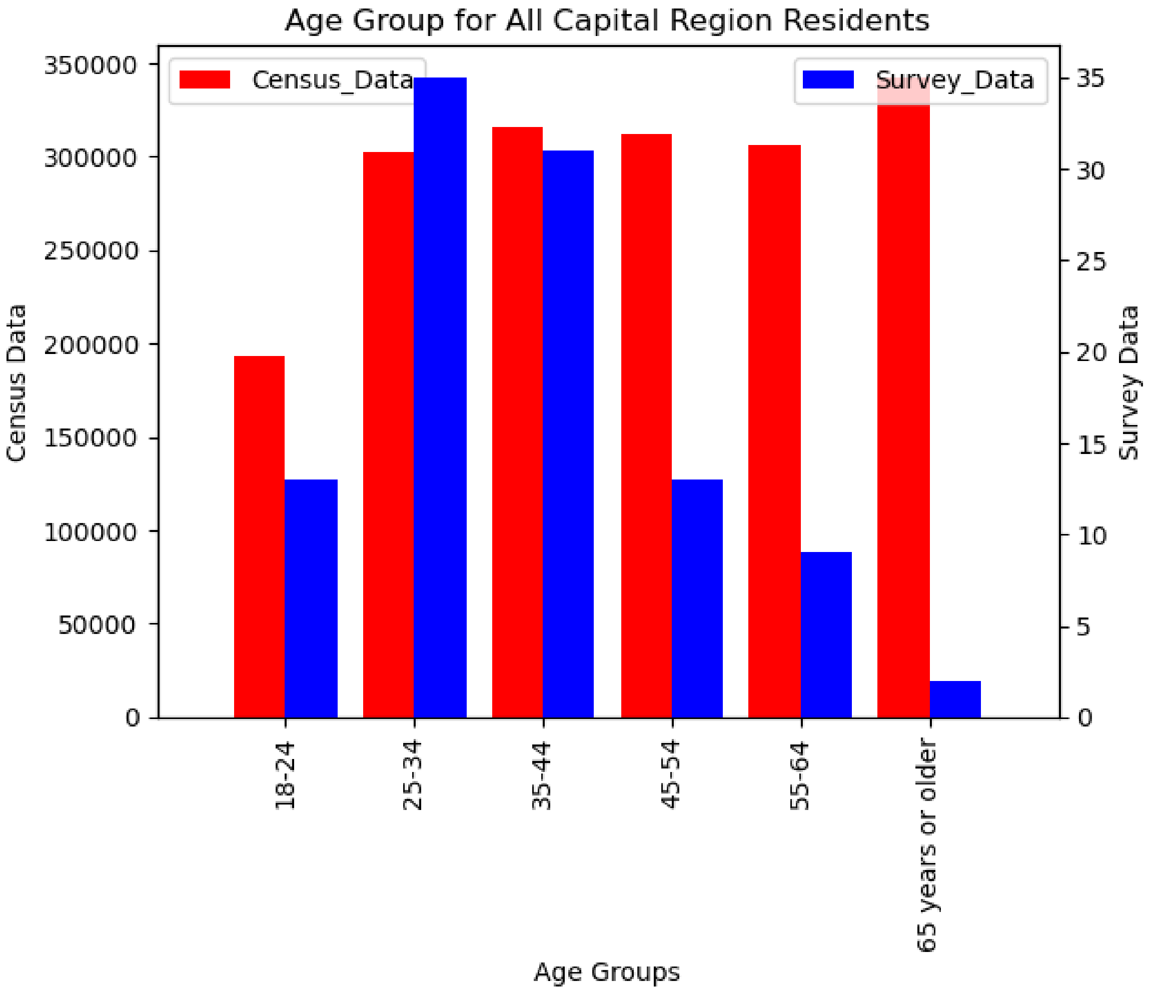


Figure B.9: Survey vs Census: Maryland Residents of Different Age Groups in the Capital Region

Total Age Per Central Maryland

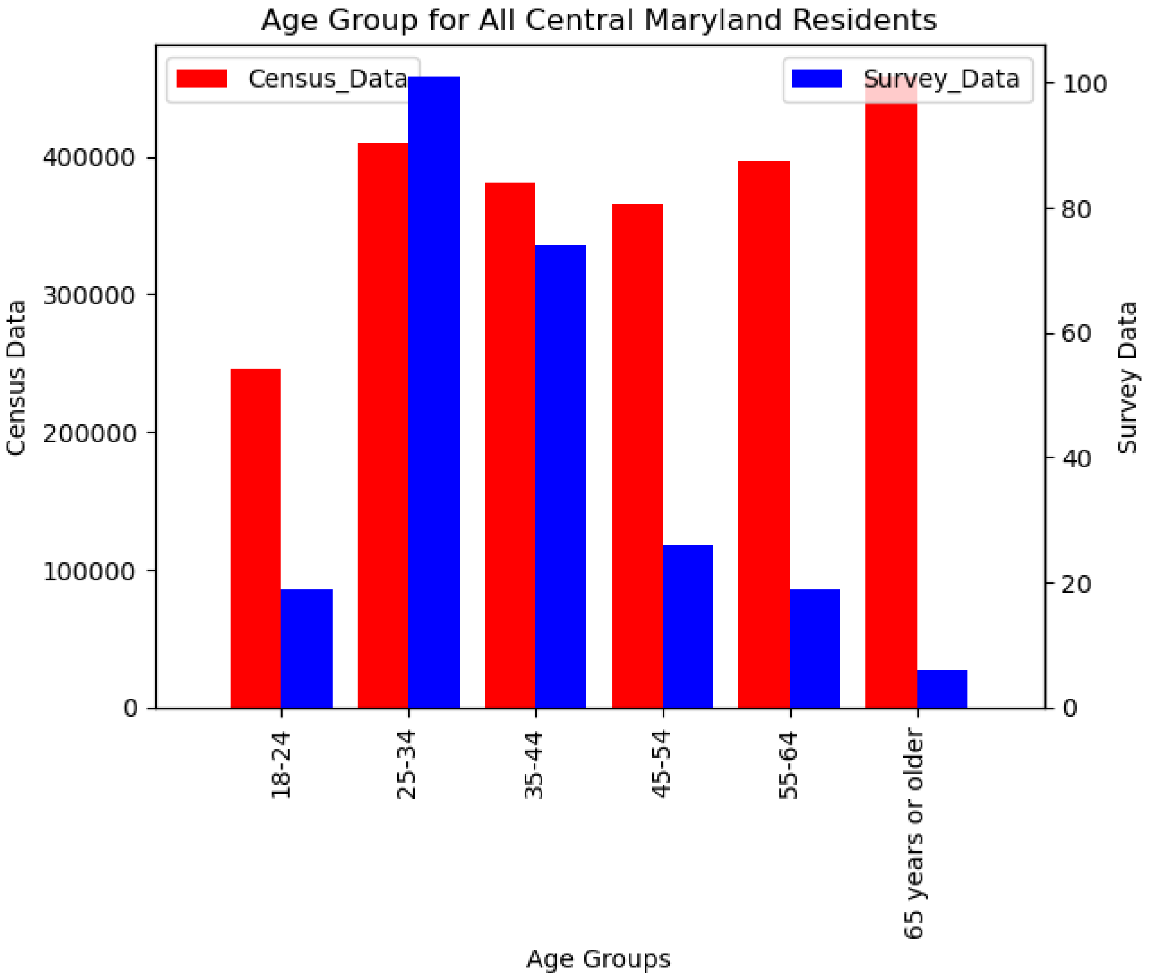


Figure B.10: Survey vs Census: Maryland Residents of Different Age Groups in Central Maryland

Total Age Per Eastern Shore of Maryland

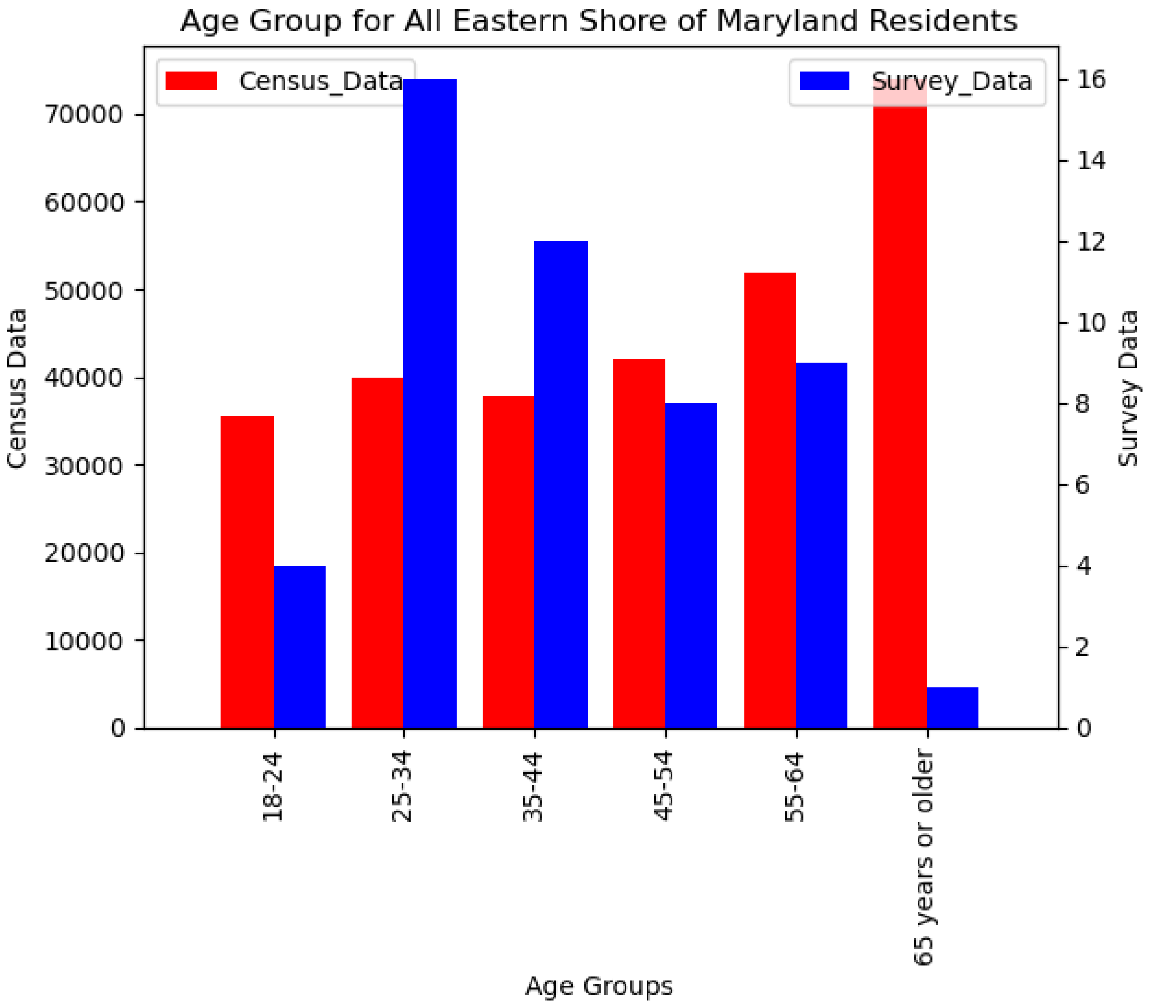


Figure B.11: Survey vs Census: Maryland Residents of Different Age Groups in the Eastern Shore of Maryland

Total Age Per Southern Maryland

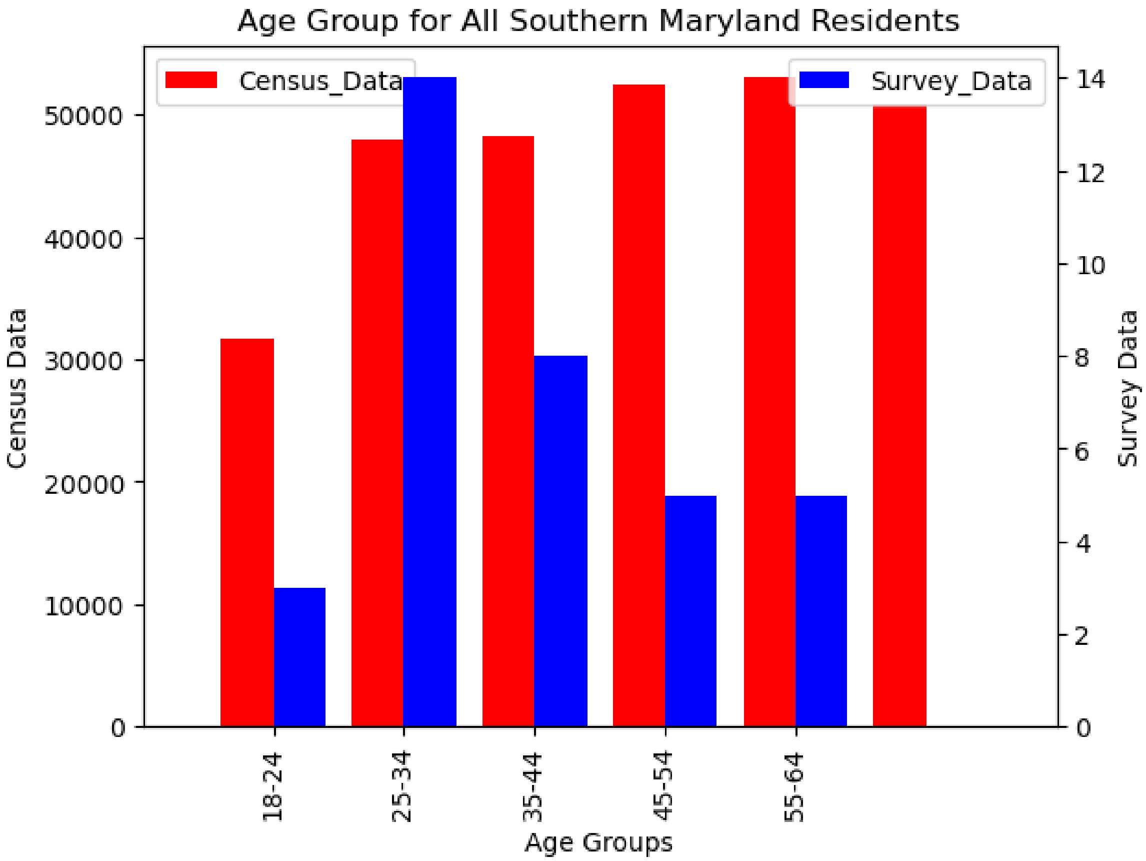


Figure B.12: Survey vs Census: Maryland Residents of Different Age Groups in Southern Maryland

B.2 Education

Numerical Y-Axis

Total Non-High School Graduates Per Maryland Region

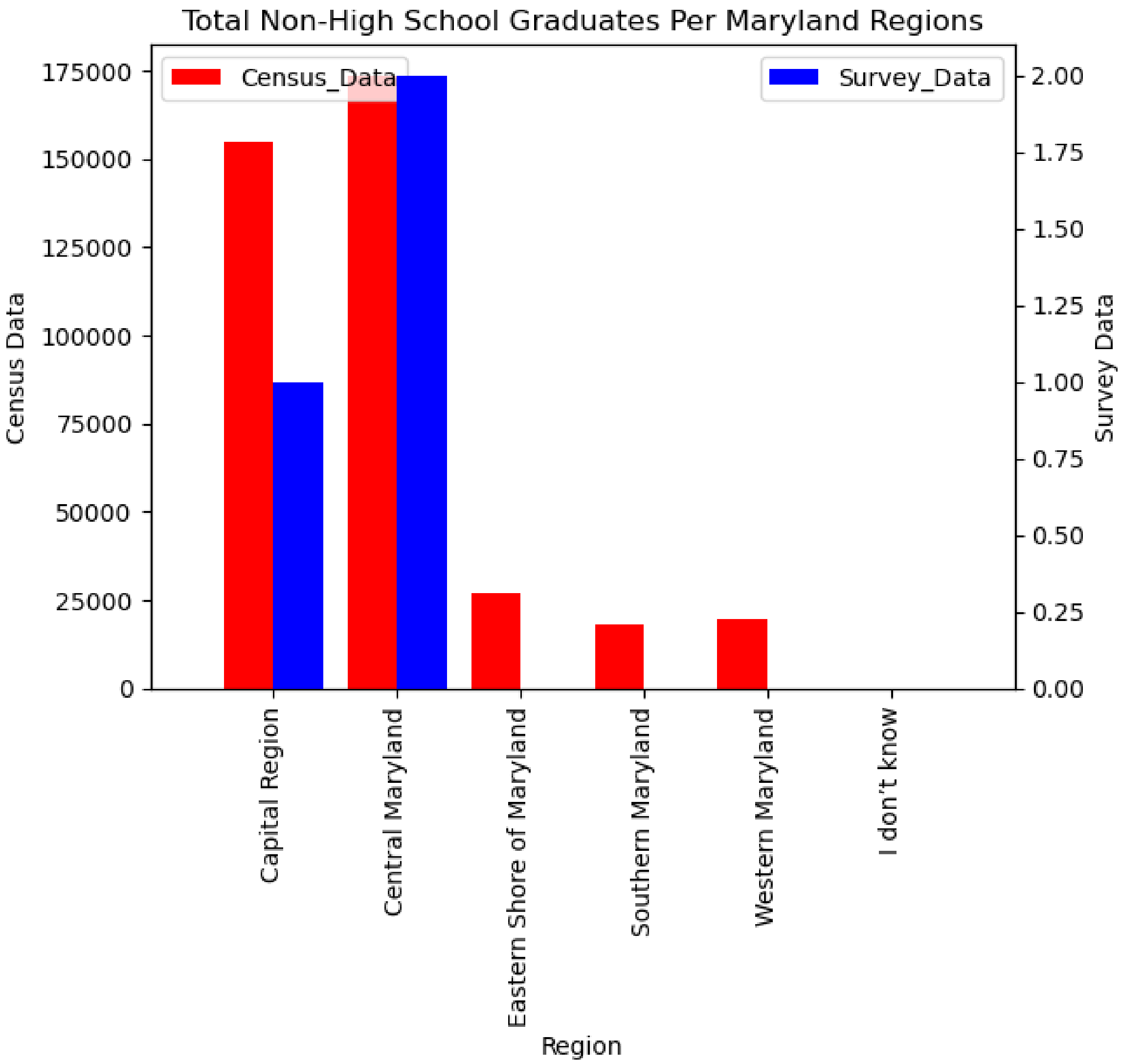


Figure B.13: Survey vs Census: Maryland Residents Without a High School Diploma by Region

Total High School Graduates Per Maryland Region

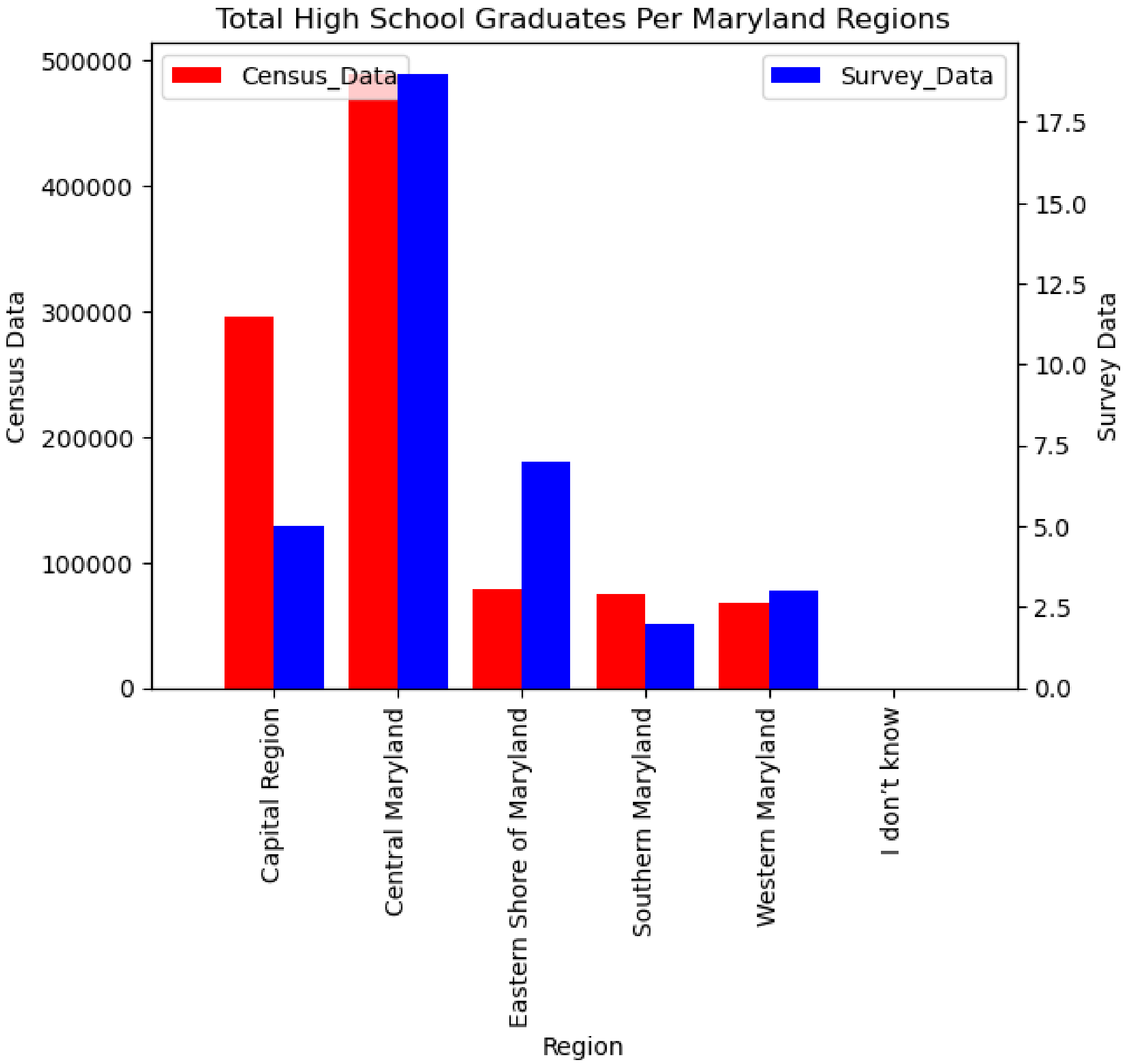


Figure B.14: Percentage of Maryland Residents with a High School Diploma by Region

Total Some College Attendees Per Maryland Region

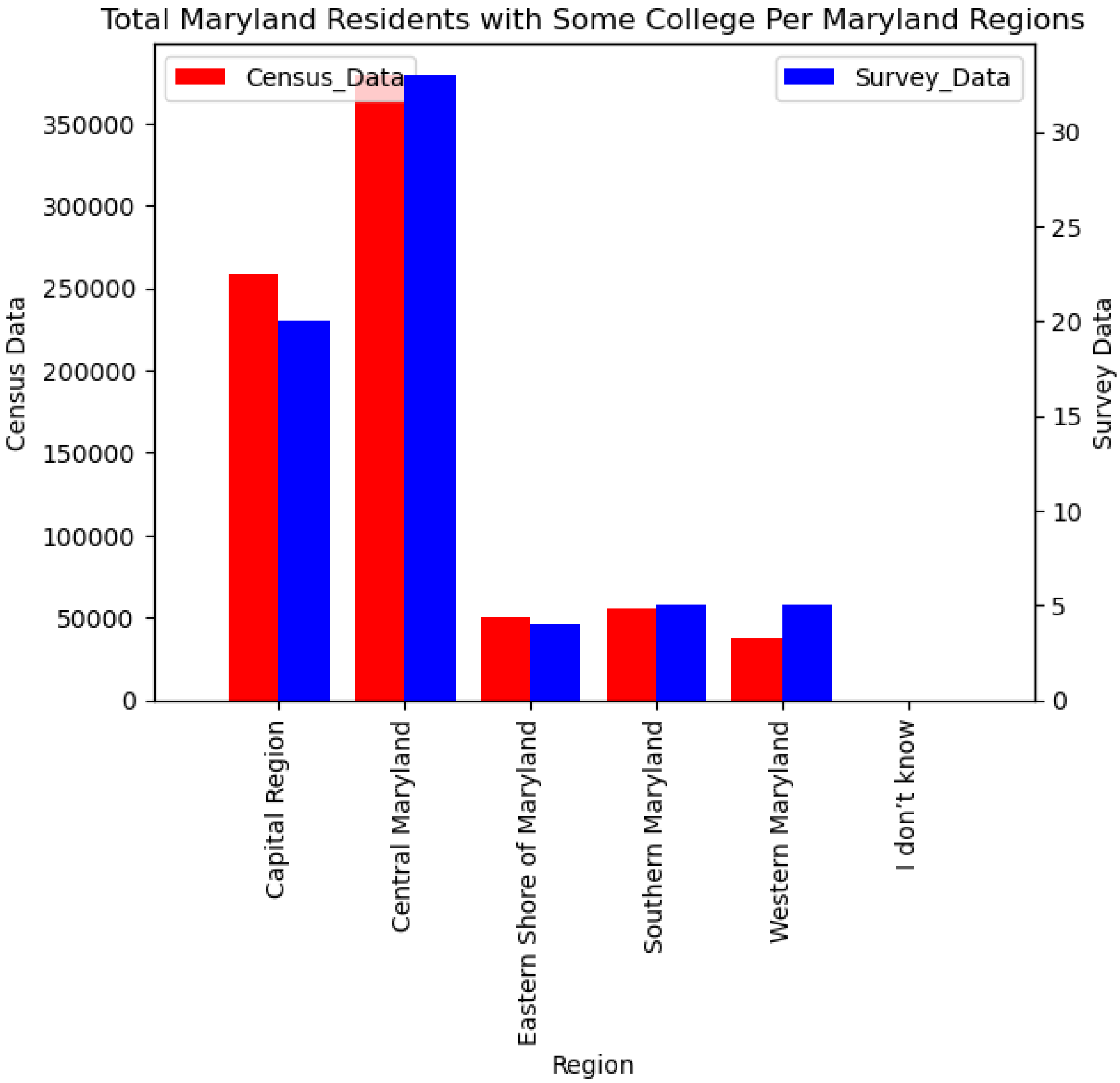


Figure B.15: Survey vs Census: Maryland Residents with Some College Education by Region

Total Associates Degree Earners Per Maryland Region

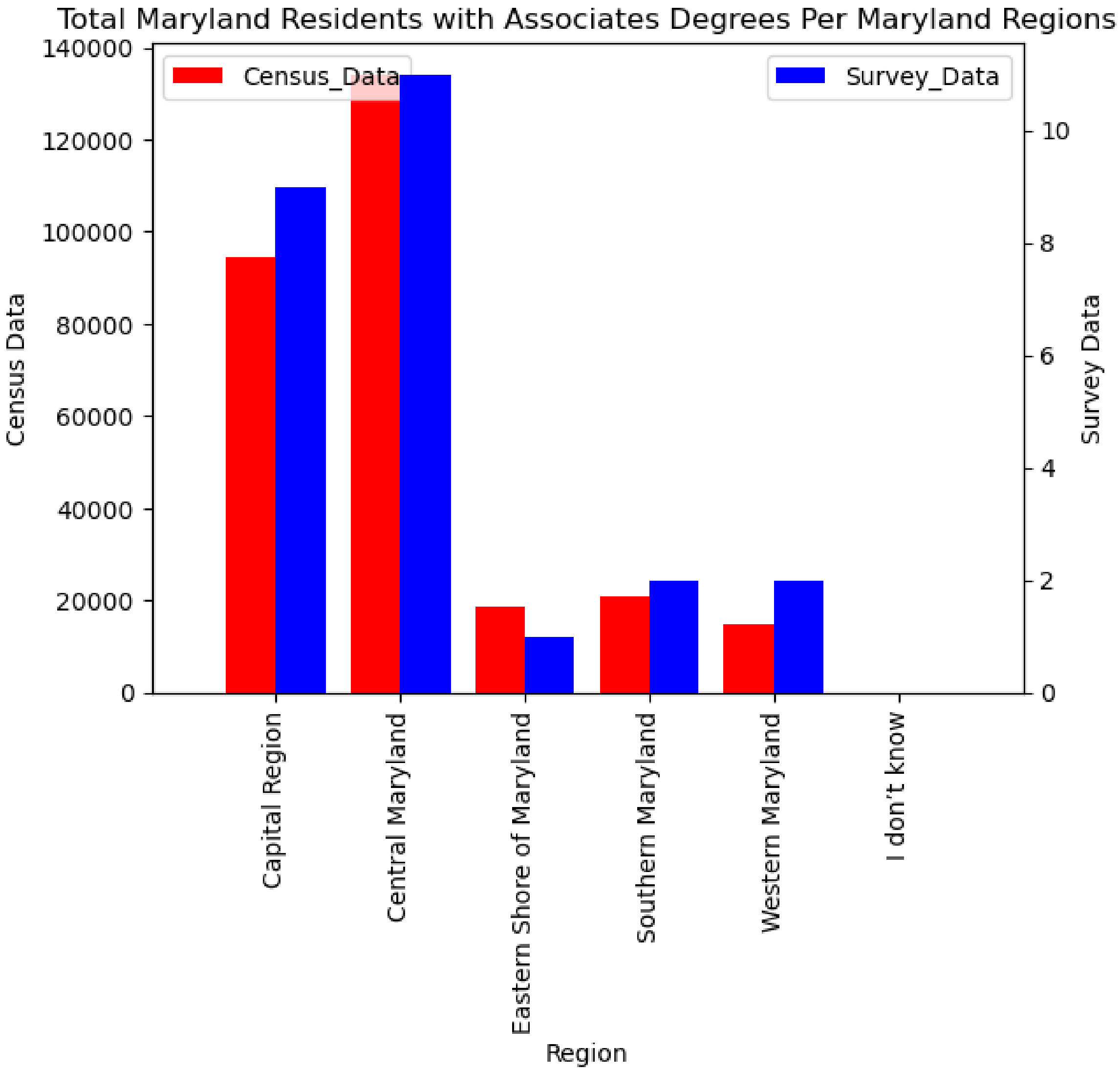


Figure B.16: Survey vs Census: Maryland Residents with an Associate's Degree by Region

Total Bachelor's Degree Earners Per Maryland Region

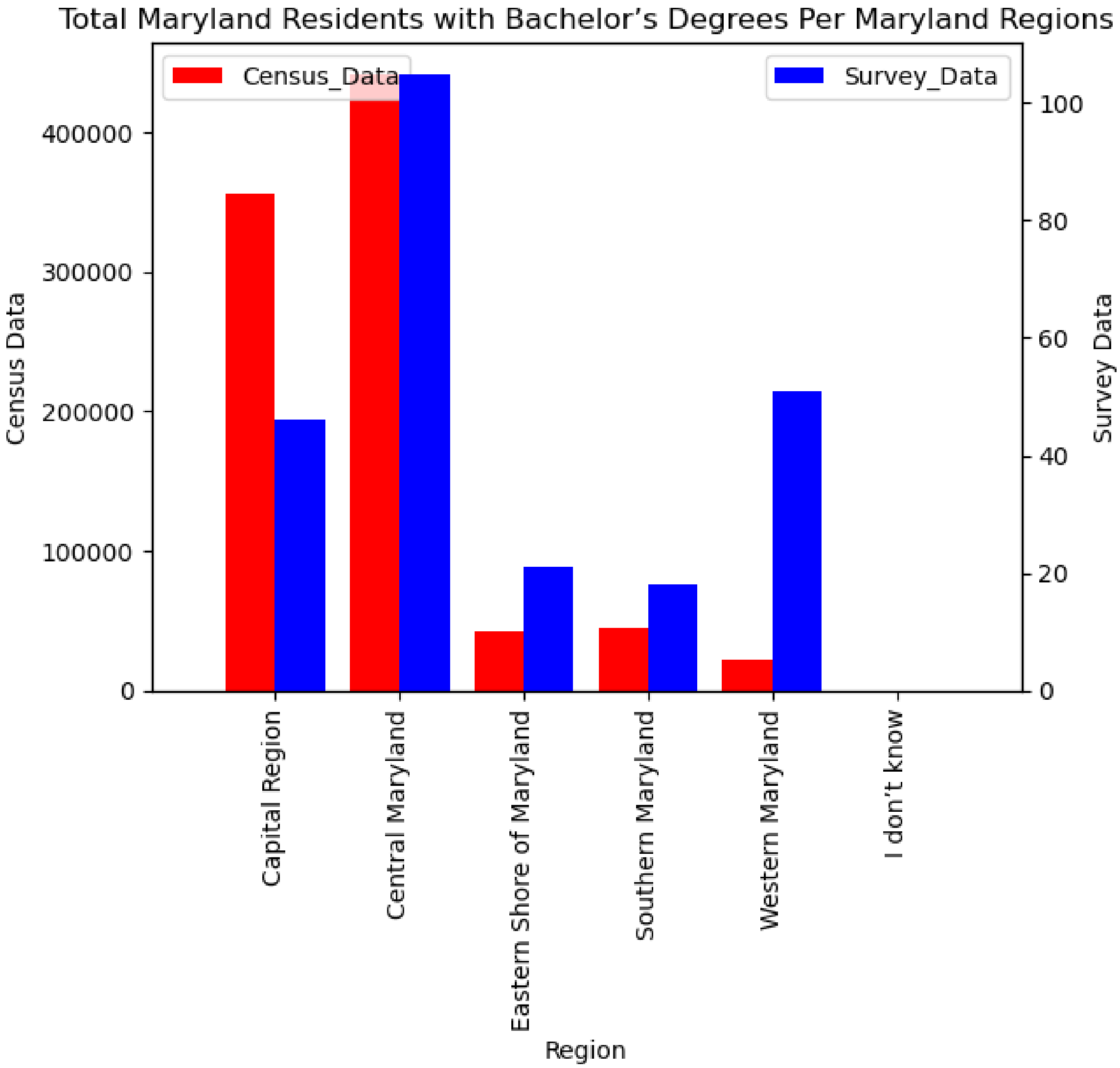


Figure B.17: Survey vs Census: Maryland Residents with a Bachelor's Degree by Region

Total Graduate Degree Earners Per Maryland Region

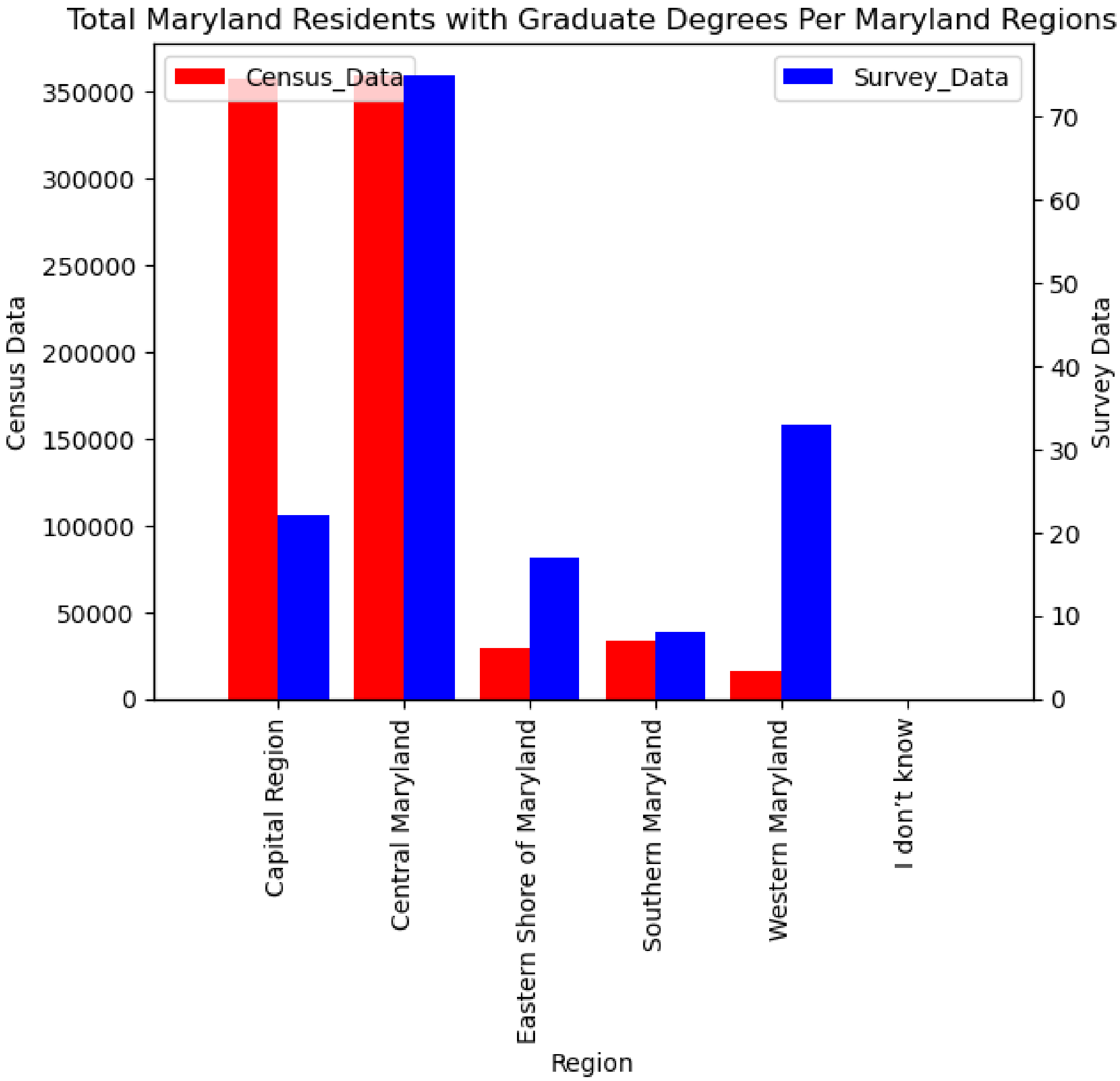


Figure B.18: Survey vs Census: Maryland Residents with a Graduate Degree by Region

Percentage Y-Axis: Education

Total Non-High School Graduates Per Maryland Region

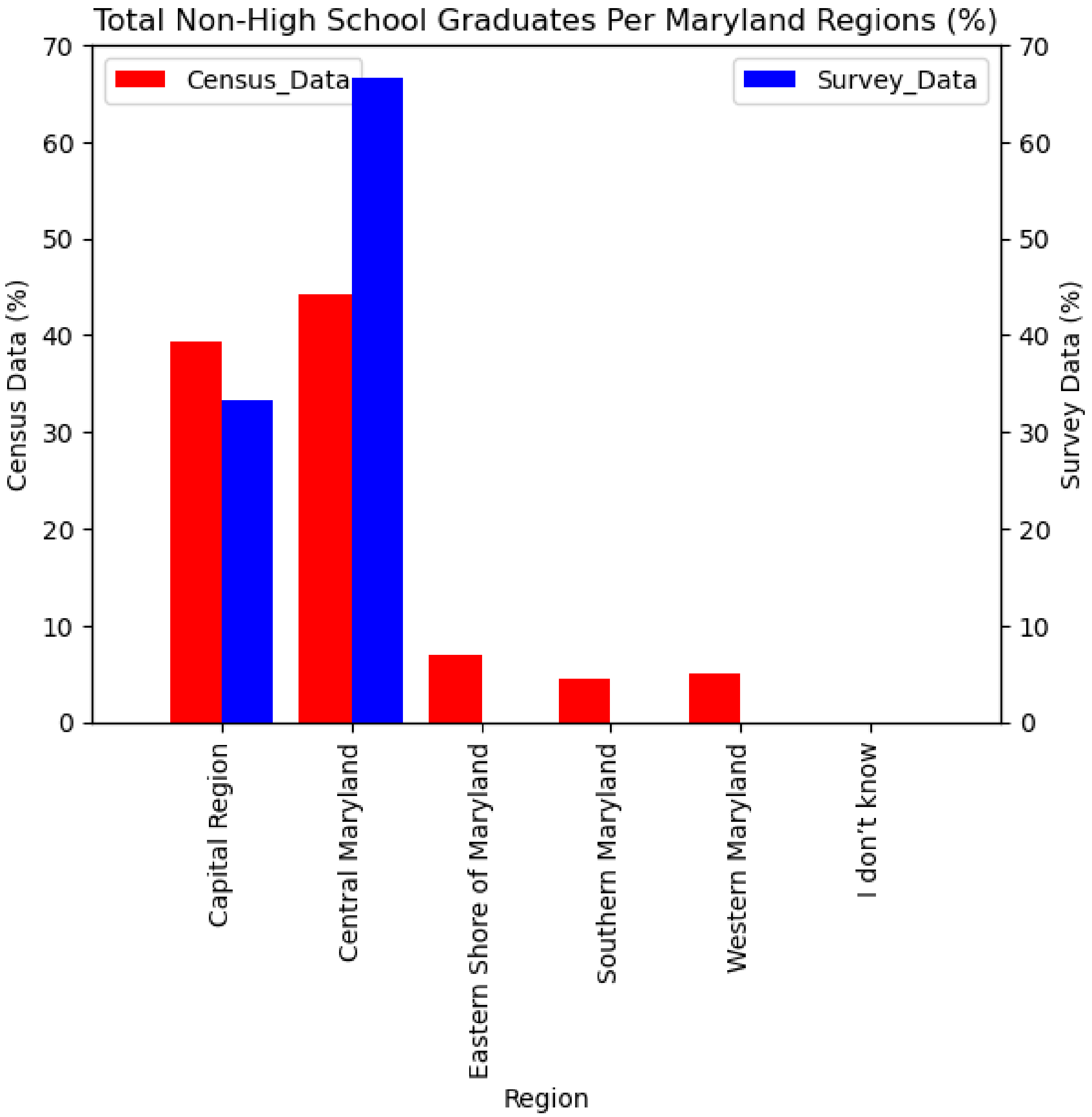


Figure B.19: Percentage of Maryland Residents Without a High School Diploma by Region

Total High School Graduates Per Maryland Region

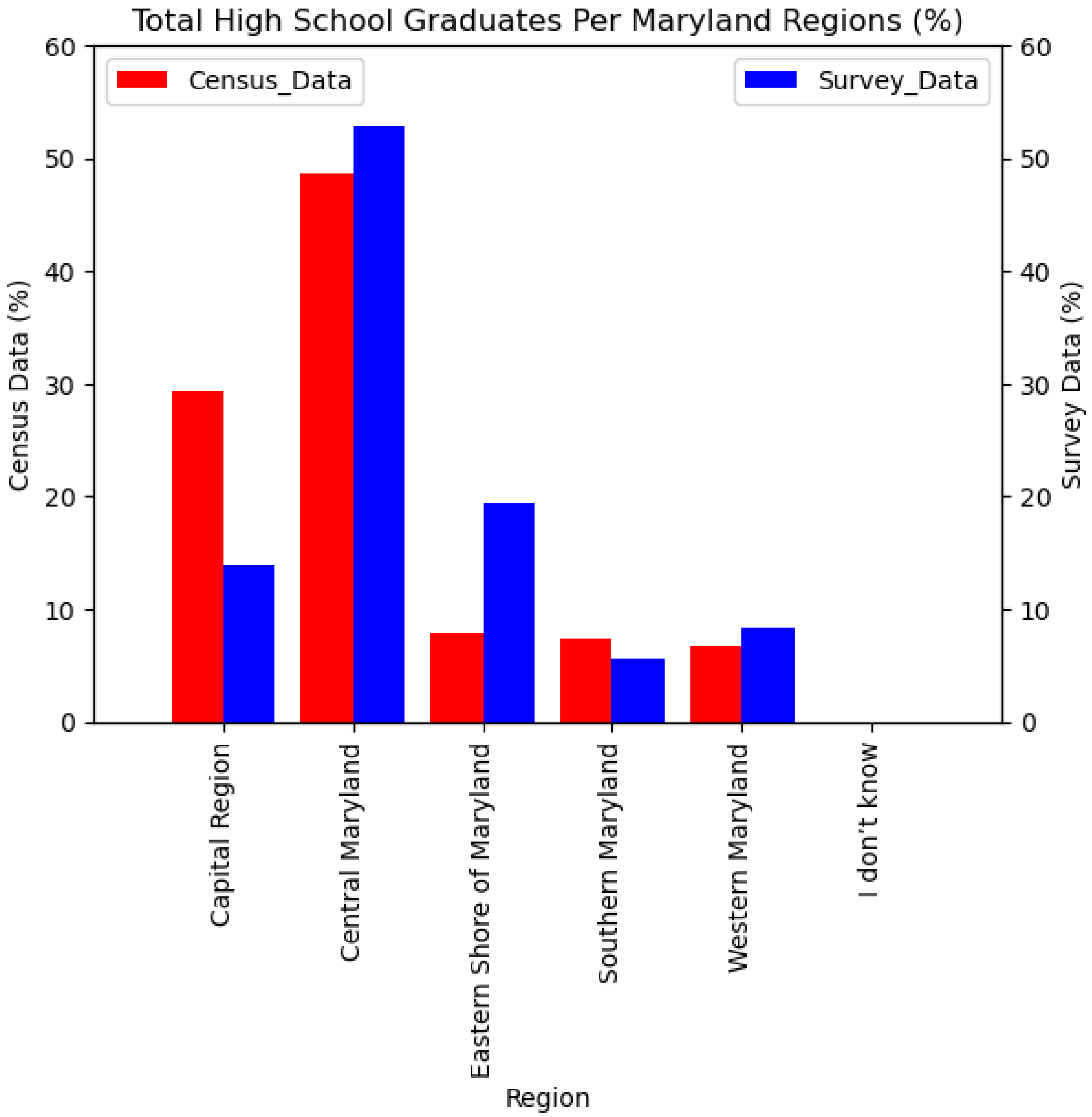


Figure B.20: Percentage of Maryland Residents with a High School Diploma by Region

Total Some College Attendees Per Maryland Region

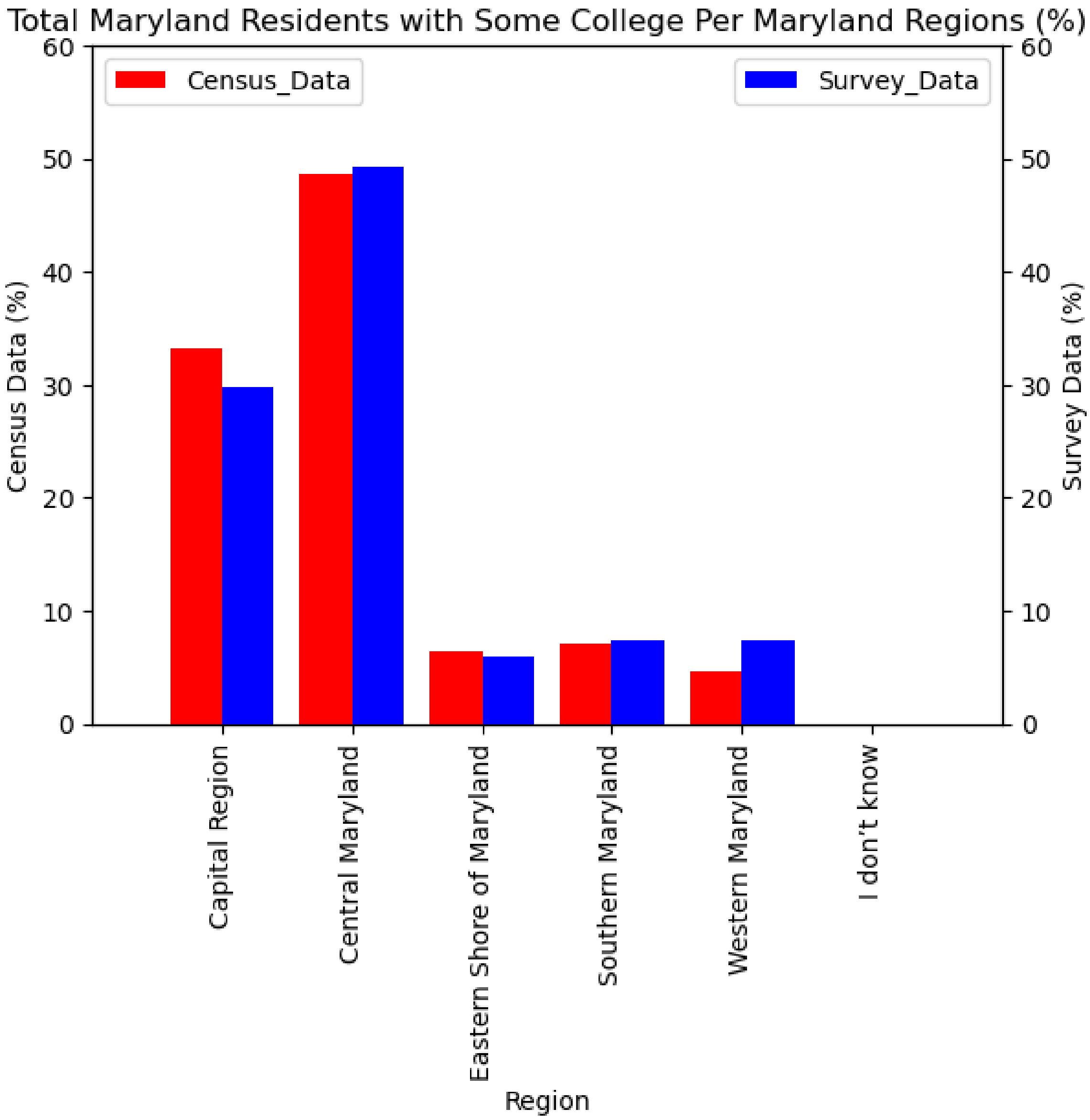


Figure B.21: Percentage of Maryland Residents with Some College Education by Region

Total Associates Degree Earners Per Maryland Region

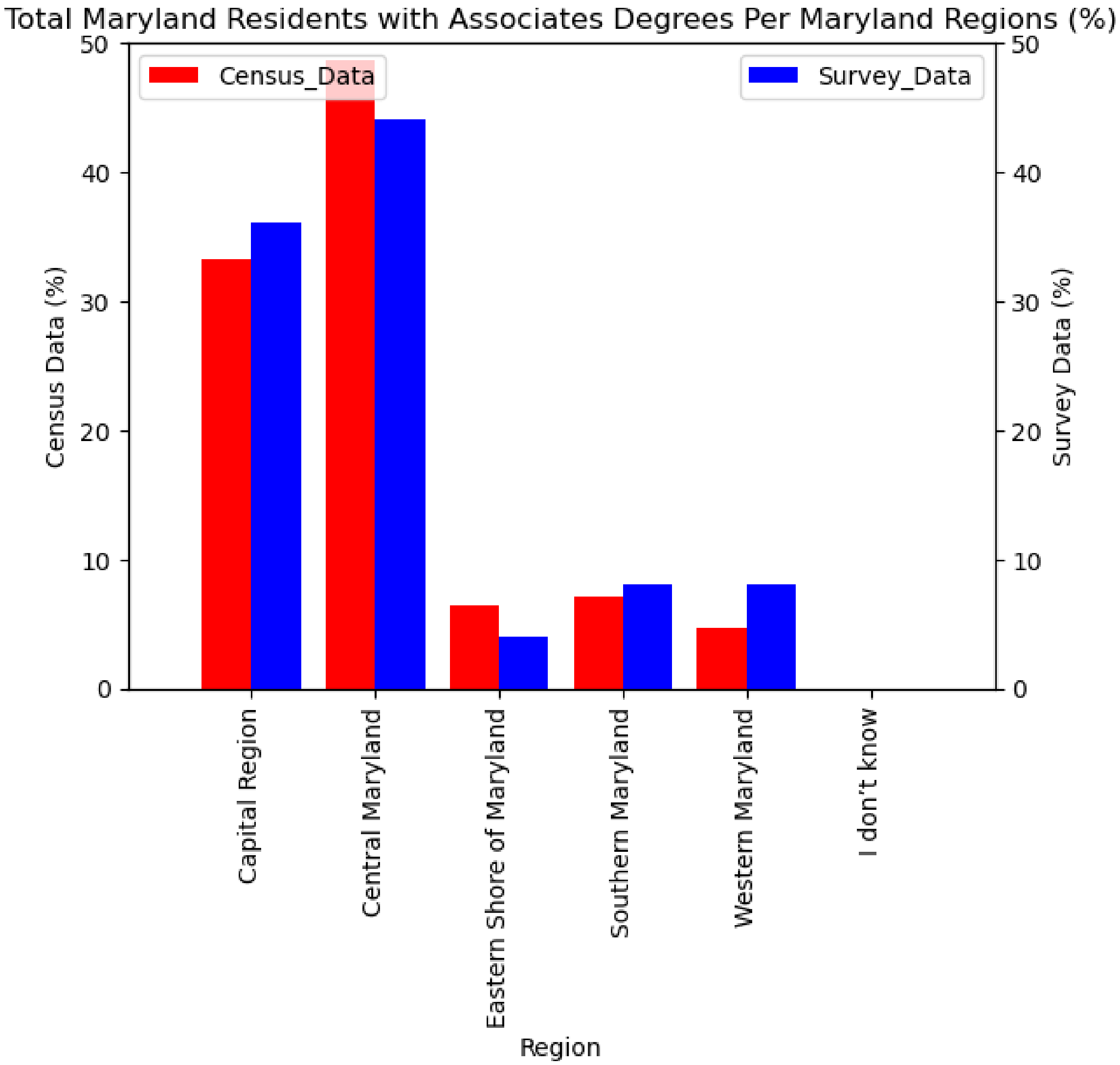


Figure B.22: Percentage of Maryland Residents with an Associate's Degree by Region

Total Bachelor's Degree Earners Per Maryland Region

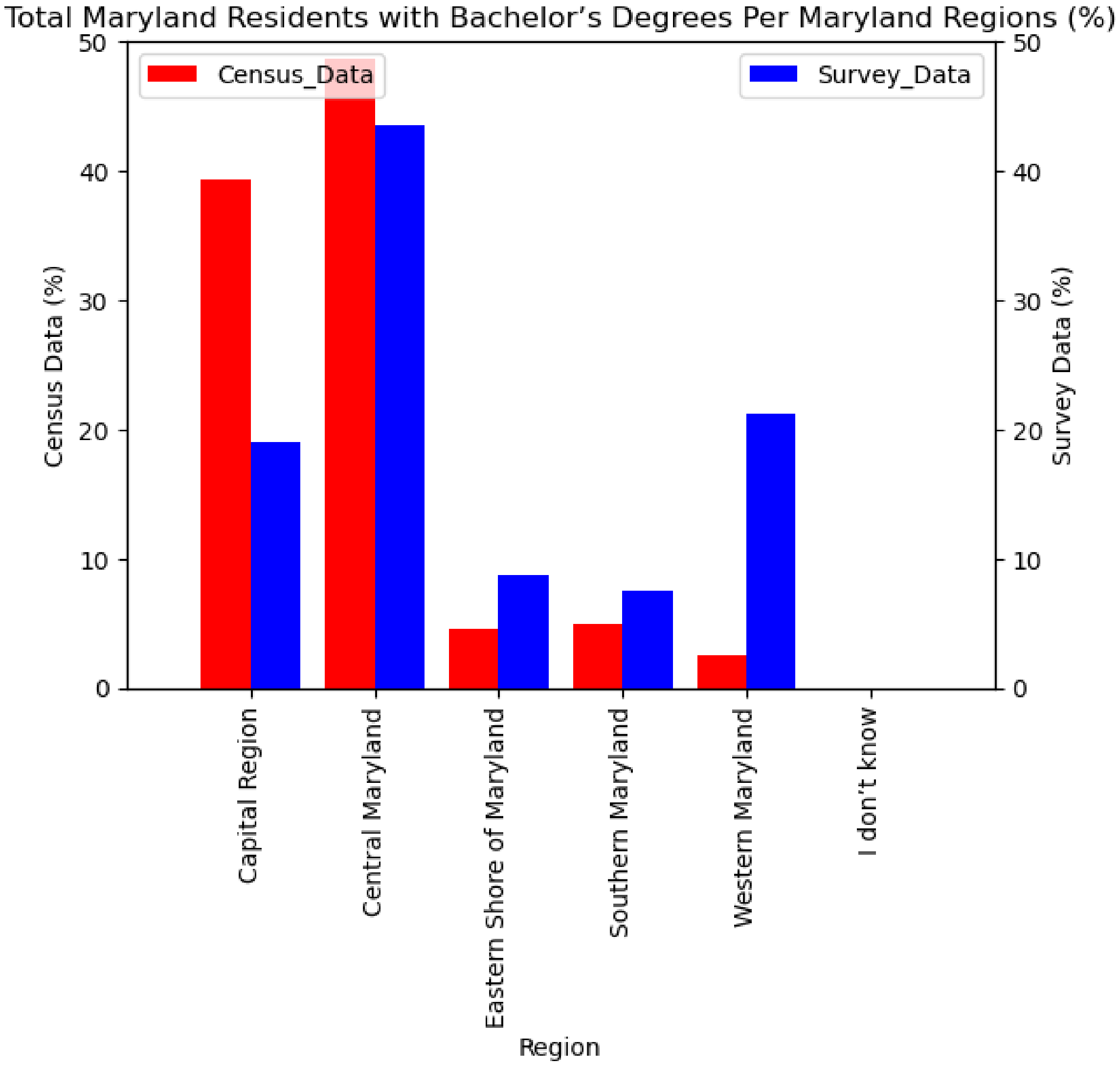


Figure B.23: Percentage of Maryland Residents with a Bachelor's Degree by Region

Total Graduate Degree Earners Per Maryland Region

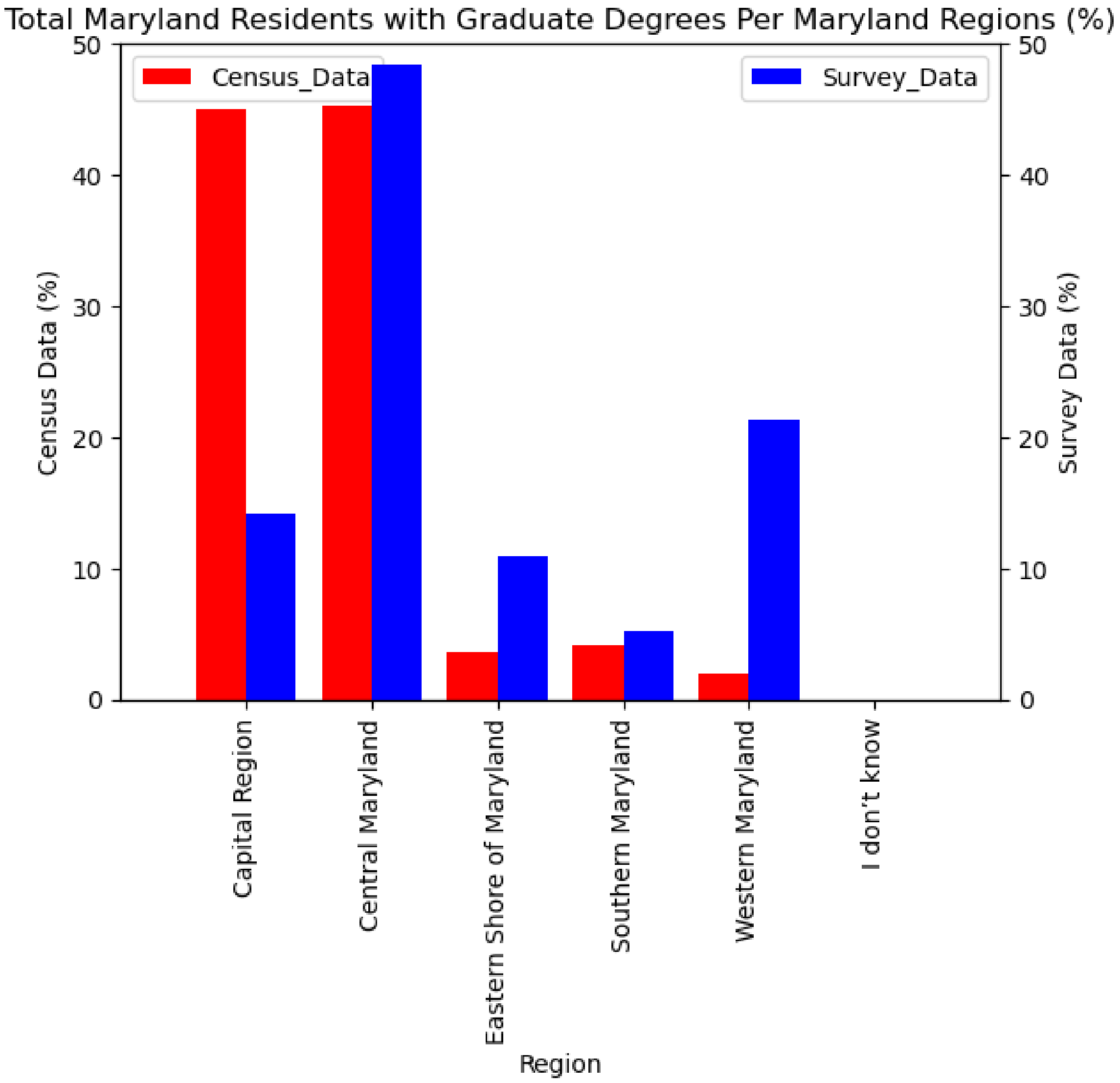


Figure B.24: Percentage of Maryland Residents with a Graduate Degree by Region

Appendix C

Survey Questions

Demographic Questions: Questions 1-4

1. Age (select one):

   - 18–24
   - 25–34
   - 35–44
   - 45–54
   - 55–64
   - 65–75
   - 75 years or older

2. Please select the jurisdiction of your primary residence:

   - Allegany County
   - Anne Arundel County
   - Baltimore City
   - Baltimore County
   - Calvert County
   - Caroline County
   - Carroll County
   - Cecil County
   - Charles County
   - Dorchester County
   - Frederick County
   - Garrett County
   - Harford County
   - Howard County

- Kent County
- Montgomery County
- Prince George's County
- Queen Anne's County
- St. Mary's County
- Somerset County
- Talbot County
- Washington County
- Wicomico County
- Worcester County
- I don't know

3. Education Level (Select One):

    - Do not have a HS Diploma or GED
    - High School Diploma or GED
    - Some College
    - Associates Degree
    - Bachelor's Degree
    - Graduate Degree
    - I don't know

4. What year were you born? (Integer field)

Backup Behavior Questions: Questions 5-7

5. How do you backup your data (Check All that apply)

    - I use a cloud service (e.g., Microsoft OneDrive, Carbonite, Google Drive)
    - I use removable storage that I keep in my house
    - I use removable storage that I keep in a location other than my house
    - I keep multiple copies of my files on my computer
    - I do not back up my data
    - I don't know

6. How often do you back up your data? (Check all that apply)

    - Continuously
    - Daily
    - Weekly
    - Monthly

- Less often than monthly but at least once a year
- Once a year or less frequently
- I do not back up my data
- I don't know

7. When was the last time you made sure your backups were valid?

   - Within a day
   - Within a week
   - Within a month
   - Within a year
   - More than a year ago
   - I do not back up my data
   - I don't know

Security Awareness Questions: Questions 8-11

8. What is Social Engineering in an information security context?

   - Any action in which someone tries to convince another person to take an action which may not be in their best interests
   - Actively trying to circumvent or get around security safeguards by finding weaknesses in a system that can be exploited without personal interaction
   - Attempting to inform people about the use of proper security policies, processes, and procedures
   - When a company makes a public announcement about something positive that has happened or is going to happen
   - I don't know

9. What is Spear Phishing?

   - When someone fraudulently sends a specifically crafted message to a person to convince them to take an action which may harm them
   - Targeted marketing emails sent to a specific person by a company based on their buying history or web browsing habits
   - When someone sends an email specifically designed to belittle the recipient
   - When someone in a business setting sends an email to a coworker inappropriately delegating their work to the recipient
   - I don't know

10. What is Phishing?

    - When someone fraudulently sends emails to people to convince them to take an action which may harm them

- When companies or individuals send out emails to promote or sell their products
- When someone you know sends an email that was forwarded to you encouraging you to forward that message on to everyone in your address book
- When someone sends an email to a large group of people and one of the recipients replies with a personal response to all recipients of the original email
- I don't know

11. What is Multifactor Authentication?

    - An additional piece of information beyond username and password which someone must provide to gain access to a system (e.g., website)
    - The frequent changing of a password so it is harder for an attacker to guess
    - Adding different numbers to the ends of a username so a user never has the same username on multiple sites
    - When someone uses a different password for each website they access
    - I don't know

Security Hygiene Questions: Questions 12, 15-18

12. Where do you use multifactor authentication? (Select one) (Grouped with other multifactor questions)

    - I do not use multifactor authentication.
    - I use multifactor authentication on my important online accounts.
    - I use multifactor authentication on most of my online accounts.
    - I use multifactor authentication wherever it is offered to me.
    - I don't know.

15. What form of multifactor authentication do you use? (Check all that apply) (Grouped with other multifactor questions)

    - I do not use multifactor authentication
    - Messages sent to my phone that contain a code
    - An application on my phone that verifies I am logging in
    - An application that generates a one-time code
    - A hardware security token (e.g., YubiKey or Google Titan)
    - I don't know.

16. How do you choose a password for your online accounts? (Check all that apply)

    - I use the same password for all of my accounts
    - I use the same password for most of my accounts
    - I use passwords that are similar but different for all of my accounts

- I use personal information (names of pets, children, or friends) as all or part of my password
- I use a unique complex password for my accounts
- I don't know

17. How do you manage the passwords for your online accounts? (Check all that apply)
    - I remember my passwords
    - I write my passwords down
    - I use a password manager
    - I don't know

History Questions: Questions 19-21, 24-28

19. Have you ever been the victim of ransomware? (Yes/No/I don't know)
20. To your knowledge, has your personal information been disclosed to unauthorized people, e.g., via a data breach? (Yes/No/I don't know)
21. Have you ever been the victim of an online scam where you lost any amount of money? (Yes/No/I don't know)
24. If so, about how much money did you lose as a victim of this scam (enter 0 if you have not lost any money)? Integer
25. Have you ever been targeted by a scammer who called you directly on the phone? (Yes/No/I don't know)
26. Have you ever lost access to any of your online accounts due to someone else taking it over? (Yes/No/I don't know)
27. Have you ever received an email claiming to be from a financial institution you use that asks you to log in to that account to resolve some issue? (Yes/No/I don't know)

Final Questions: Questions 29, 31

29. How likely do you think you are to be targeted by a malicious actor (Hacker) at some time in the future? (5-point scale + I don't know)
30. I am very confident with my computer skills. (5-point Agree/Disagree scale)
31. I am knowledgeable about cybersecurity. (5-point Agree/Disagree scale)

List of Abbreviations

ISI	Johns Hopkins University Information Security Institute
MTurk	Amazon Mechanical Turk