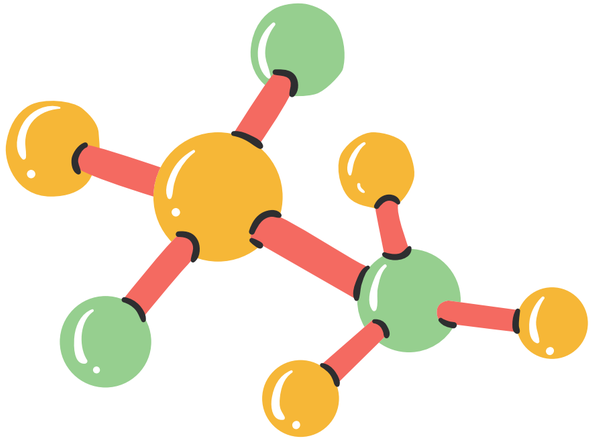
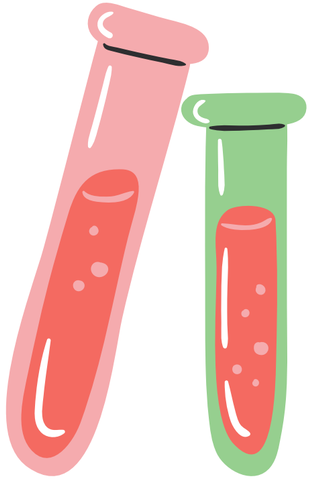
RESEARCH METHODOLOGY





OUR TEAM

1. Upasana Yadav-
86092300015

2.Heena Gagwani-
86092300022

3.Bhavesh Pashte -
86092300001

4.Vinayak Khithani-
86092300019

5.Arisha Akhtar-
86092300042

Research Problem Statement

Crafting a Focused Approach to Enhance Cybersecurity Awareness for Social Media, Mobile, Software Security and Online Privacy, Empowered by Statistical Computing.

- Over the years, the threats of attacking a system and stealing its data has increased. Our project aims to identify the steps a user should be taking to secure himself / herself.

- Emphasizing software security brings attention to the importance of secure coding practices, vulnerability management, and the role of software updates in mitigating potential risks.

- The affect of Machine Learning algorithms in cybersecurity domain. Understanding how Data Poisoning can manipulate the algorithm’s output and how one can avoid it.

- Analyzing the awareness among people about cybersecurity attacks

Analytical:

•Reporting current developments in cyber security domain.
• Analyzing awareness of cybersecurity among common people, whether people are aware about cybersecurity threats.

One Time:

•Research is done one time: over the current data available and current developments happening.
•Also, analzying how the present will affect the future.

Applied Research:

1. Our research will identify gaps in citizen's knowledge about cybersecurity.

2. After identifying those gaps, we aim to built a website addressing those gaps and how to tackle them

1.CYBERSECURITY, DATA PRIVACY AND BLOCKCHAIN

APA: Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... & Platts, J. (2022). Cybersecurity, data privacy and blockchain: a review. SN Computer Science, 3(2), 127.

- This paper focuses on conducting experiments related to detecting, capturing, processing, and storing data. The ISO 27001 management system plays a vital role in ensuring the security of communications, protocols, and control mechanisms for data access.

- Data is gathered through blockchain by various users, then passes through a system layer including ISO 27001, smart contracts, and GDPR. It is subsequently transferred to an administrator. Cloud technology supported by cybersecurity, employs methods like big data analytics, visualization, and IoT. Finally, data storage is initiated via blockchain.

By Upasana Yadav (86092300015)

- This paper focuses on conducting experiments related to detecting, capturing, processing, and storing data. The ISO 27001 management system plays a vital role in ensuring the security of communications, protocols, and control mechanisms for data access.

- Data is gathered through blockchain by various users, then passes through a system layer including ISO 27001, smart contracts, and GDPR. It is subsequently transferred to an administrator. Cloud technology supported by cybersecurity, employs methods like big data analytics, visualization, and IoT. Finally, data storage is initiated via blockchain.

By Upasana Yadav (86092300015)

2. The Urgency of Cyber Security in Secure Networks

APA: Mehta, S., Sharma, A., Chawla, P., & Soni, K. (2021, May). The urgency of cyber security in secure networks. In 2021 5th international conference on intelligent computing and control systems (ICICCS) (pp. 315-322). IEEE

- The paper highlights the importance of cyber security in today's world and the need to protect personal data while using the internet, doing online transactions, or online shopping. It provides overview of cyber security and the types of cyber-attacks that can occur.

- The paper provides insights into the emerging threats in the field of cyber security, such as social engineering, mobile malware, and botnets, and suggests strategies to counter them.

By Arisha Akhtar (86092300042)

- It emphasizes the need for developers to ensure the security of theirapplications/websites and adopt secure Internet and reliable systems to protect user privacy.

- It suggests that the development of global-scale identity management and traceback techniques can enable the detection of cyber attackers and protect cyberspace infrastructure and information.

- The practical implications of this paper are that it can help individuals, organizations, and governments to understand the importance of cyber security and adopt strategies to protect their data and infrastructure from cyber-attacks.

By Arisha Akhtar (86092300042)

3. DATA PROTECTION AND CYBER LAWS IN INDIA

APA: A. Halder, D., & Jaishankar, K. (2021). Cyber governance and data protection in India: A critical legal analysis. In Routledge Companion to Global Cyber-Security Strategy (pp. 337-348). Routledge.

B. Shairgojri, A. A., & Dar, S. A. (2022). Emerging Cyber Security India's Concern and Threats. International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290, 2(04), 17-26.

- In the digital age, security, safety and privacy are of paramount importance to a leading country like India.

- Huge amount of personal & sensitive data of citizens, different government entities is being stored and maintained by government.

By Bhavesh Pashte (86092300001)

- There are some projects, policies, cyber laws and amendments made to safeguard personal data from cyberattacks.

1. National Critical Information Infrastructure Protection Centre (NCIPC)
2. National Cyber Coordination Centre (NCCC)
3. National Cyber Security Policy (2013)
4. Information Technology Act (2000)
5. Information Technology (Amendments) Act (2008)

- Even though Indian government has made provisions to protect data, there were cases of data leakage, invasion of privacy, cyber terrorism in the past years.

- The Govt should emphasize proper auditing of data retained and stored by stakeholders & the existing laws must be properly implemented and executed in order to fortify national security.

By Bhavesh Pashte (86092300001)

4. Cyber-attacks on major companies and analysis of the attacks

APA: A. Quader, F.; Janeja, V.P., Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies, J.Cybersecure. Priv. 2021, 1, 638–659.

B. Suman Acharya, Sujata Joshi, Impact Of Cyber-Attacks On Banking Institutions In India : A Study Of Safety Mechanisms And Preventive Measures, Palarch's Journal Of Archaeology Of Egypt/Egyptology, 17(6), ISSN 1567-214x.

- It is clear that the ubiquitous nature of connectivity and the constant movement of data intensify cyber dangers. From the analysis of various cyber-attacks on the companies, it came to our notice that human behavioral aspects and the response to malicious stimuli are the weakest link in a successful cyber-attack.
- The authors bought to the notice the importance of classifying the cyber-attacks into various categories such as financial impacts, non-financial impact, number of customers impacted, cultural factors, end-user trust and loyalty, etc due to which we understood about the intentions of the attackers and we can make mitigation strategies for future scenarios.

By Vinayak Khithani (86092300019)

- In the next paper, authors are trying to show us the gap in cyber security by making us understand the two cyber-attacks on the renowned banks of India.

- First cyber-attack: The UBI 2017 cyber-attack was a classic phishing attack, originating from an email disguised as from the RBI. The malicious code entered bank's network and servers, causing a $170 million theft attempt. The main reason for this attack is a lack of awareness and proper training for officials to identify and prevent cyber-attacks.

- Second cyber-attack: A malicious cyber-attack on Cosmos Bank of Pune in August 2018 compromised the bank's internal and ATM infrastructure, causing false payment transfers and ATM withdrawals using 450 cloned debit cards. The attack resulted in 84 crores of rupees theft, breaking defense layers. Cybercriminals may have researched Cosmos bank's infrastructure and background surveillance system and hence regular auditing of bank generated reports should not have been ignored.

By Vinayak Khithani (86092300019)

- Both the papers examines cyber threats and real-world case studies to identify key factors affecting their propagation. We understood that ignorance and negligence are main human factors, education, IT security policies, social engineering, internal threats and non-up-to-date technology are the main factors of cyber-attacks. To protect against cyber threats, proactive investment and prioritization are crucial.

By Vinayak Khithani (86092300019)

5. CYBERSECURITY: PRESSING PRIORITY OF INDIA

APA: Tejpal, K., Vidyapeeth, D. P., Pimpri, P., & Patole, J. (2023). CYBERSECURITY: PRESSING PRIORITY IN INDIA. The Online Journal of Distance Education and e-Learning, 11(2).

- With everything today getting connected, the data of people (in form of Banks accounts, Aadhar Card, Pan Card, Online transactions, Online Shopping) is at huge risk. Not just data, but the insights one can get about the market, about the people, about their spending behaviour, and many more. This research paper helps us understand the entire scenario of cybersecurity in India.
- Through this paper, we come to know that cybersecurity knowledge is essential for not only businesses, governments but also individuals.
- Cybersecurity comprises of Application Security, Information Security, Network Security, Operational Security and End User Education.

By Heena Gagwani (86092300022)

- Following are the challenges that authors talk about in Cybersecurity:

1. Cyberterrorism
2. Digital Data Threat
3. Cyberwarfare
4. Cyberinfrastructure Concerns
5 .Lack of experts
6. Lack of Co-ordination

- Methods of Attack Possible:

1. Phishing
2. Malware
3. Denial of Service
4. SQL Injection Attack
5. Drive by Attack
6. Password Attack
7. Man in Middle Attack
8. Eavesdropping Attack
9. Cross – Site Scripting Attack

By Heena Gagwani (86092300022)

- After explaining different cybersecurity components, challenges in India to cybersecurity and methods of attack, author explains about the need for cybersecurity in India.
- Looking at the data, from 2010 to 2020, the cybercrime rates in India have increased by a huge percent. With online businesses developing, authors explain that network security is going to be most crucial.
- With keeping this in mind, there are certain cybersecurity initiatives in India which are:

  1. Cert – In 2. Cyber Surakshit Bharat 3. National Cyber Security Strategy
  4. Cyber Swachhta Kendra 5. National Critical Information Infrastructure Protection Centre

- India's Legal Framework: First Act in cybersecurity regulation was passed in 2000. Since then various laws such as IT Act 2008, IT Rules 2011, Indian SPDI Rules 2011, National Cyber Security Policy, 2013, IT Rules, 2011, Reserve Bank of India Act 2018 has been formed.

By Heena Gagwani (86092300022)

- The findings were:

1. Significant gap of cybersecurity professionals
2. With rapid digitization, there is need of rigid laws
3. Low Awareness among the citizens

- Conclusion:

1. Cybersecurity should be introduced as a compulsory subject in high schools and colleges. Awareness campaigns for citizens should be held to teach them about the measures to be taken to safeguard their data.
2. There should be a comprehensive cybersecurity policy in India.
3. The collaborations between public and private sectors must be strengthened.

By Heena Gagwani (86092300022)

4. Investment in Research to learn about AI powered cyberattacks, defence against AI powered cyberattacks, how to mitigate data poisoning issues in AI.

- The research gap?

A pinpoint solution to a particular problem in cybersecurity domain must be given. This research paper was based on entire scenario of cybersecurity in India. A thorough investigation in each of the law, in each sector – public and private is required.

By Heena Gagwani (86092300022)

What is Hypothesis?

A hypothesis is a precise, testable statement of what the researcher predicts will be the outcome of the study. It is stated at the study's beginning. Typically, this entails putting forth a potential correlation between the independent and dependent variables. A hypothesis must be able to be put to the test against reality and either be confirmed or disproven.

HYPOTHESIS 1

Null Hypothesis:
Software security and Mobile security has no significant effect on cybersecurity awareness

Alternate Hypothesis:
Software security and Mobile security has a significant effect on cybersecurity awareness

HYPOTHESIS 2

Null Hypothesis:

No correlation exists between an individual's level of social media engagement / their knowledge about victims to social engineering attacks and the awareness they have.

Alternate Hypothesis:

A correlation exists between an individual's level of social media engagement / their knowledge about victim to social engineering attacks and the awareness they have.

HYPOTHESIS 3

Null Hypothesis

There is no significant relationship between the frequency of application updates and the level of cybersecurity awareness among users.

Alternate Hypothesis:

The frequency of application updates is associated with a higher level of cybersecurity awareness, with users who update their applications more often being more security-conscious.

HYPOTHESIS 4

Null Hypothesis:
People’s awareness about cyber security and their concern about digital/online privacy are not associated..

Alternate Hypothesis:
People’s awareness about cyber security and their concern about digital/online privacy are associated..

Sample data to test each of the hypothesis

- We aim to collect primary data for each of the hypothesis through google forms.

- For each of the hypothesis, we will be setting different kinds of questions and will be performing statistical analysis to find out whether there exists an association or not.

RESEARCH DESIGN

Sampling Design:

We aim to collect data by circulating questionnaires. Our aim is to divide the sample into different age groups.
Age groups: Less than 20, 20 to 35, 35 to 59, 60 or above.

Sampling Method: Simple Random Sampling

Questionnaires: Questionnaires are circulated through google forms.

RESEARCH DESIGN

Statistical Design: We aim to conduct following tests:

- Correlation Test
- Test of Validity
- Test of Reliability
- Test of Feasibility
- Chi-square Test

Pilot Survey Questionnaire

Q1. How many hours per day on average do you spend on social media platforms?

Objective: To gain insights about the time user spends on social media .

Q2. Are the password that you use to access your bank account more complex than the password used to access your social accounts?

Objective: To highlight the importance of using stronger and more complex passwords for bank accounts due to the higher security risk and potential financial consequences associated with them, compared to social media accounts.

Pilot Survey Questionnaire

Q3. Have you ever received suspicious friend request from individuals who claim to be affiliated with reputable organizations or businesses?

Q4. Have you received messages from contacts claiming to be in urgent need of financial assistance on social media?

Objective: Identity theft has been more common in recent years, and the attackers sometimes seek for money or pose as officials from trusted businesses using their false identities. These methods are used to access users personal information and prepare attacks. The objective of this question is to study data and, if possible, establish a link between an individual's online behaviour and their likelihood of becoming a target of a cyberattack.

Pilot Survey Questionnaire

Q5. Do you use any additional security features or apps on your mobile device, such as antivirus software or VPNs?

Objective: Aim is to gather information about whether respondents proactively install and use additional security software or apps,such as antivirus programs ,virtual private networks(VPNs),Two Factor Authentication or Application Lock on their mobile devices.This can help assess their awareness and commitment to mobile device security.

Q6. My applications/software are automatically updated with no intervention from me _____ and I usually _____ any permission request from the application/software.

Objective: The first blank helps determining if you prefer to stay up-to-date with the latest features and security patches or if you prefer manual control over updates.
Whereas the second blank relates to how you handle requests for access to your device's features, such as camera, microphone, location, etc.

Pilot Survey Questionnaire

Q7. Have you ever received cybersecurity training or education in your workplace or educational institution?

Objective: Cybersecurity is a critical concern in today's digital age, and understanding an individual's level of expertise in this area can be important for assessing their ability to protect sensitive information, identify potential threats, and mitigate security risks.

Q8. Have you ever sought professional help for mental health related issues due to growth of technology? (or due to not being able to cope up due to technology)

Objective: Understanding if the growth of technology or the threats of it are causing people to seek professional help.

Pilot Survey Questionnaire

Q9. How do you store the email id's, passwords, bank account number and UPI pins? Please describe

Objective: Aim is to recognize how passwords are stored. Are they encrypted or not? Are they just written down or remembered? Creating a word cloud of the description to determine what is the most common way and hence also implying whether the person knows about cybersecurity prevention measures or not.
Also performing text analysis to understand how passwords are being saved.

Q10. Are you really concerned about your online privacy / digital data protection?

Pilot Survey Questionnaire

Q10. Are you really concerned about your online privacy / digital data protection?

Objective: The objective behind asking this question is to engage in a discussion about online privacy and data protection, raise awareness about these important issues, and understand the user's perspective and concerns regarding their own online privacy.

Pilot Survey Questionnaire

Q11. If we create an all around approach for protecting against these threats, would you be willing to learn?

Objective: Understanding whether people are open to learn about cybersecurity prevention attacks or not.

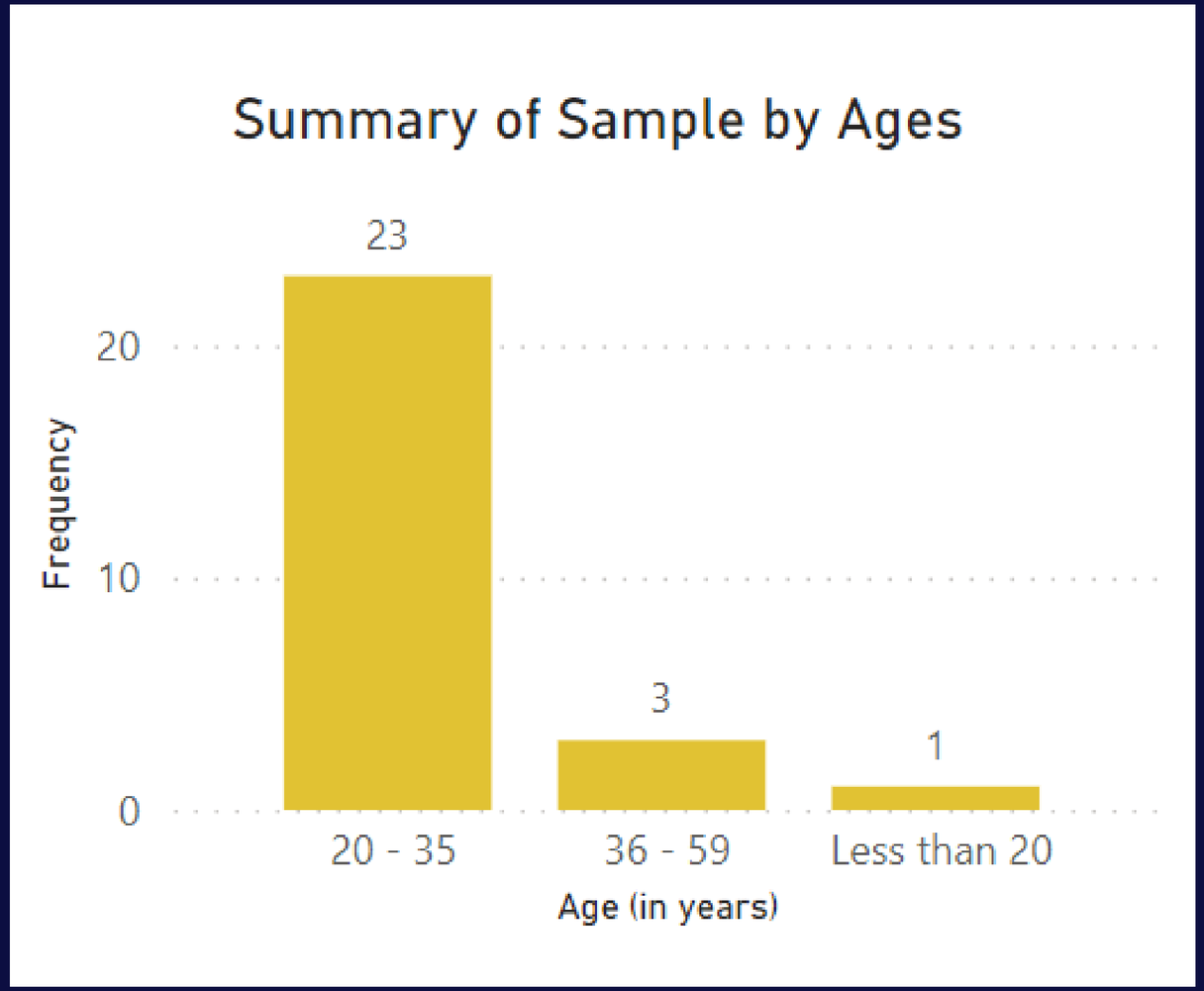
If we do get a positive response, we would be creating a website where user can explore ways to secure data on devices better.

PFA (Google Form)

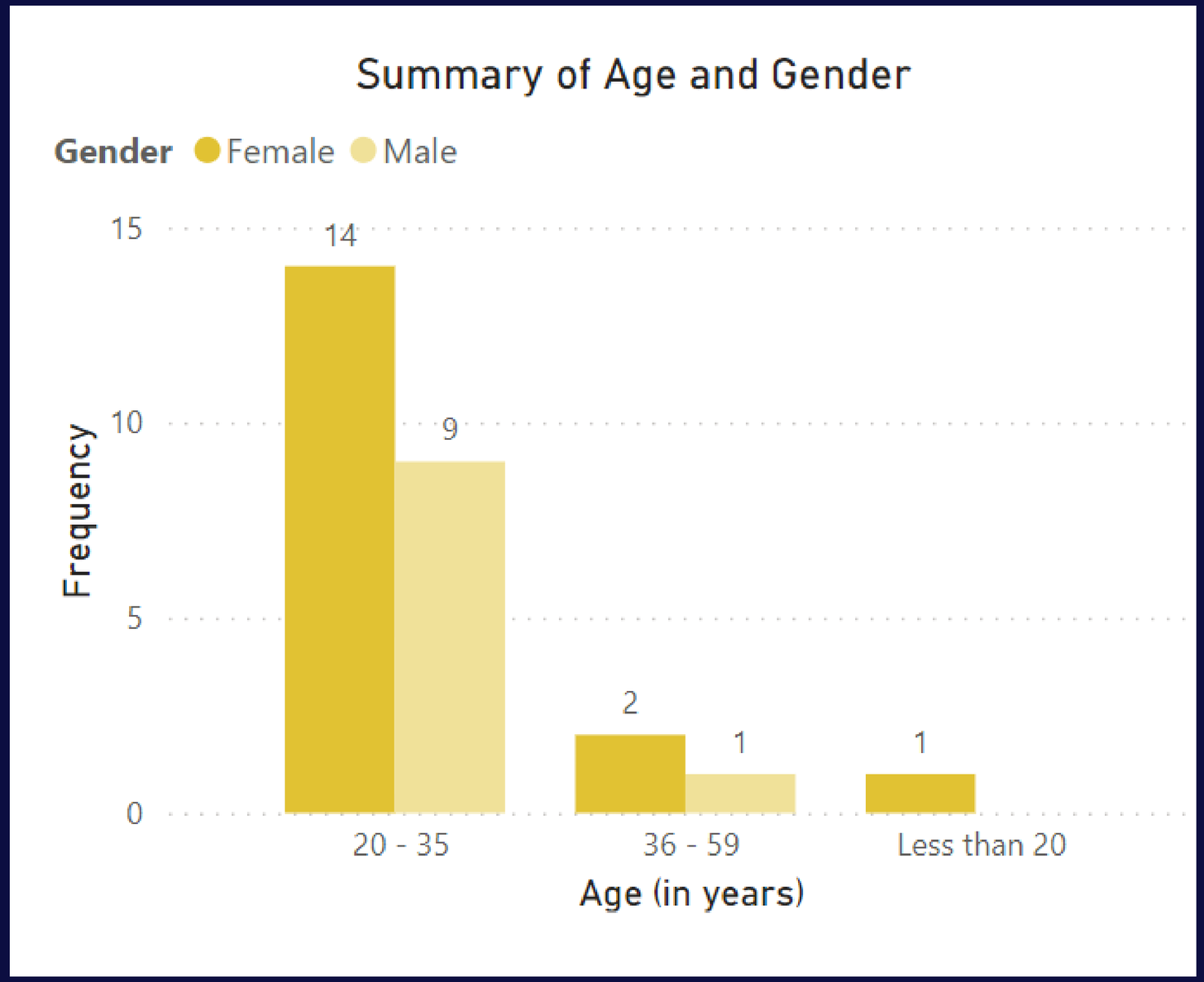
Pilot Data Summary

Sample Size: 27

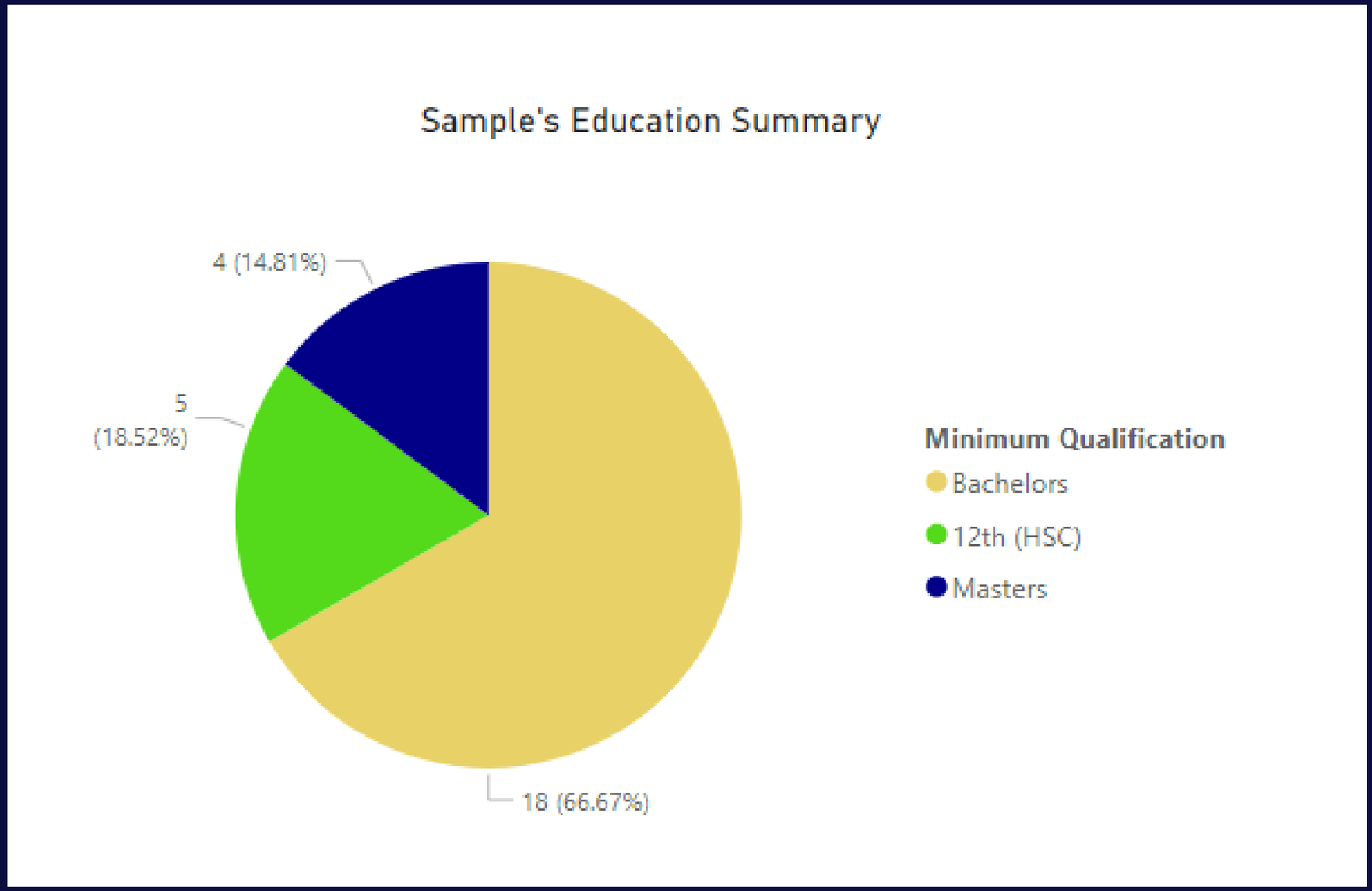
Age Groups:



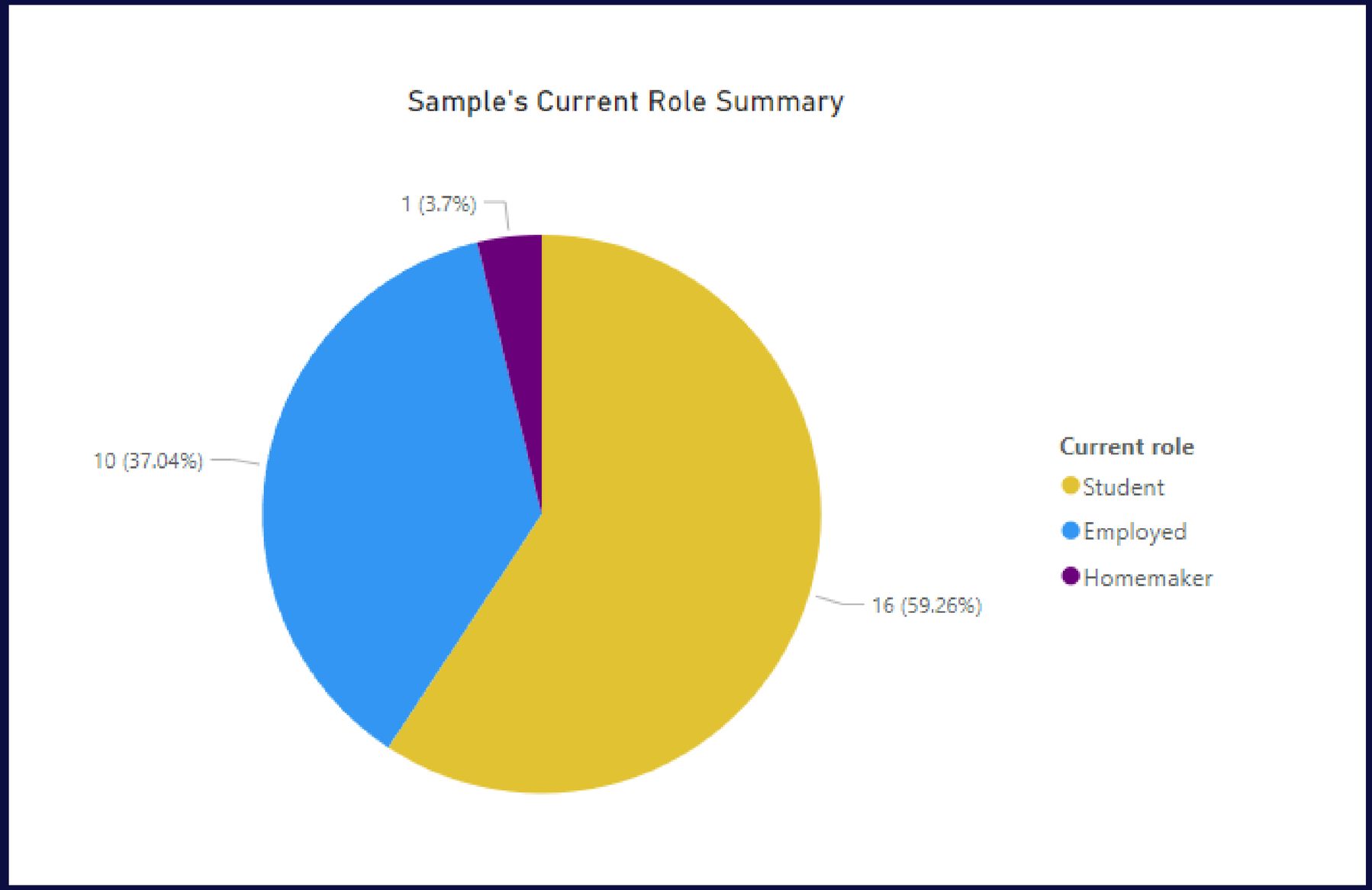
Age Groups and Gender:



Sample’s Education Summary:

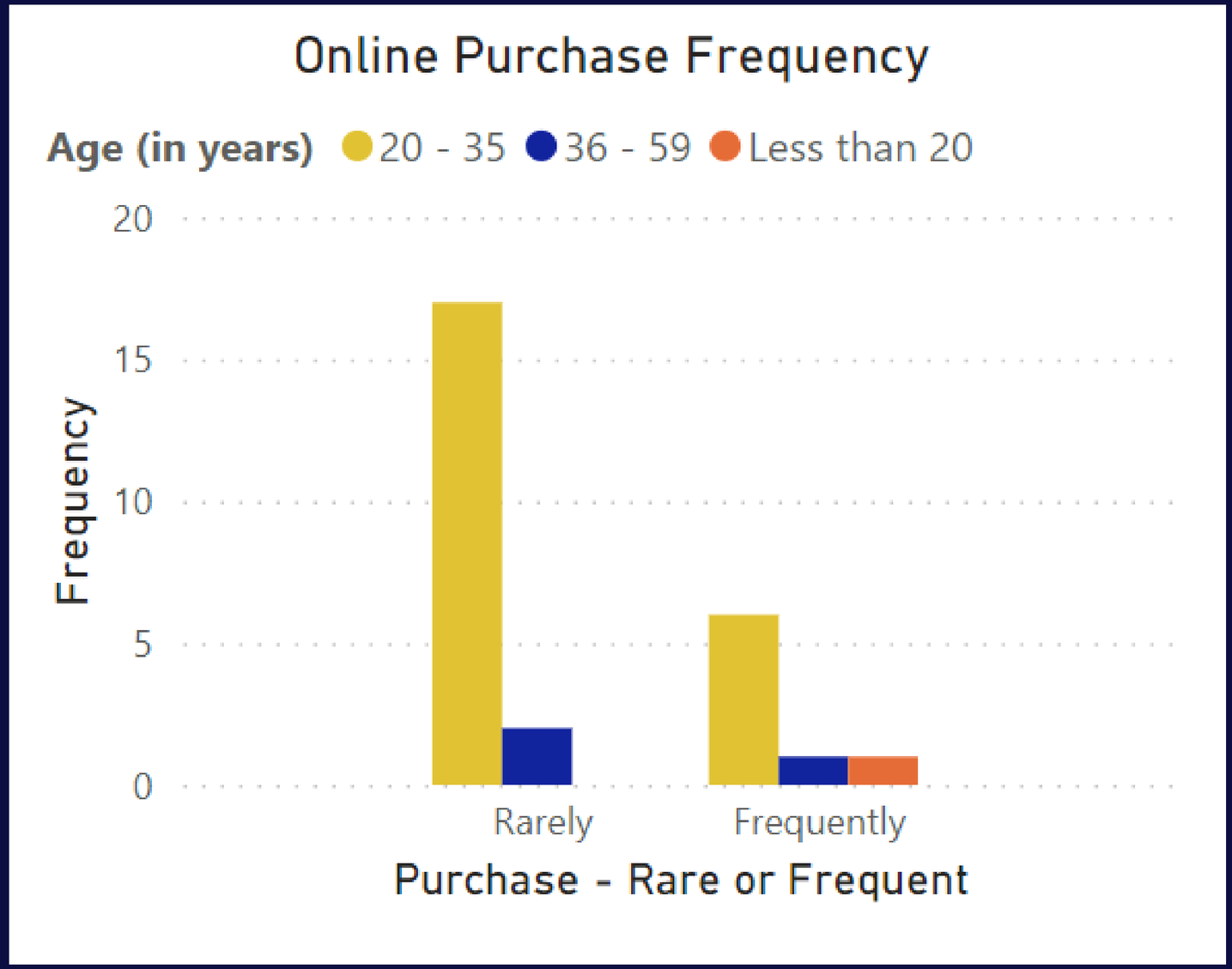


Sample’s Current Role Summary:

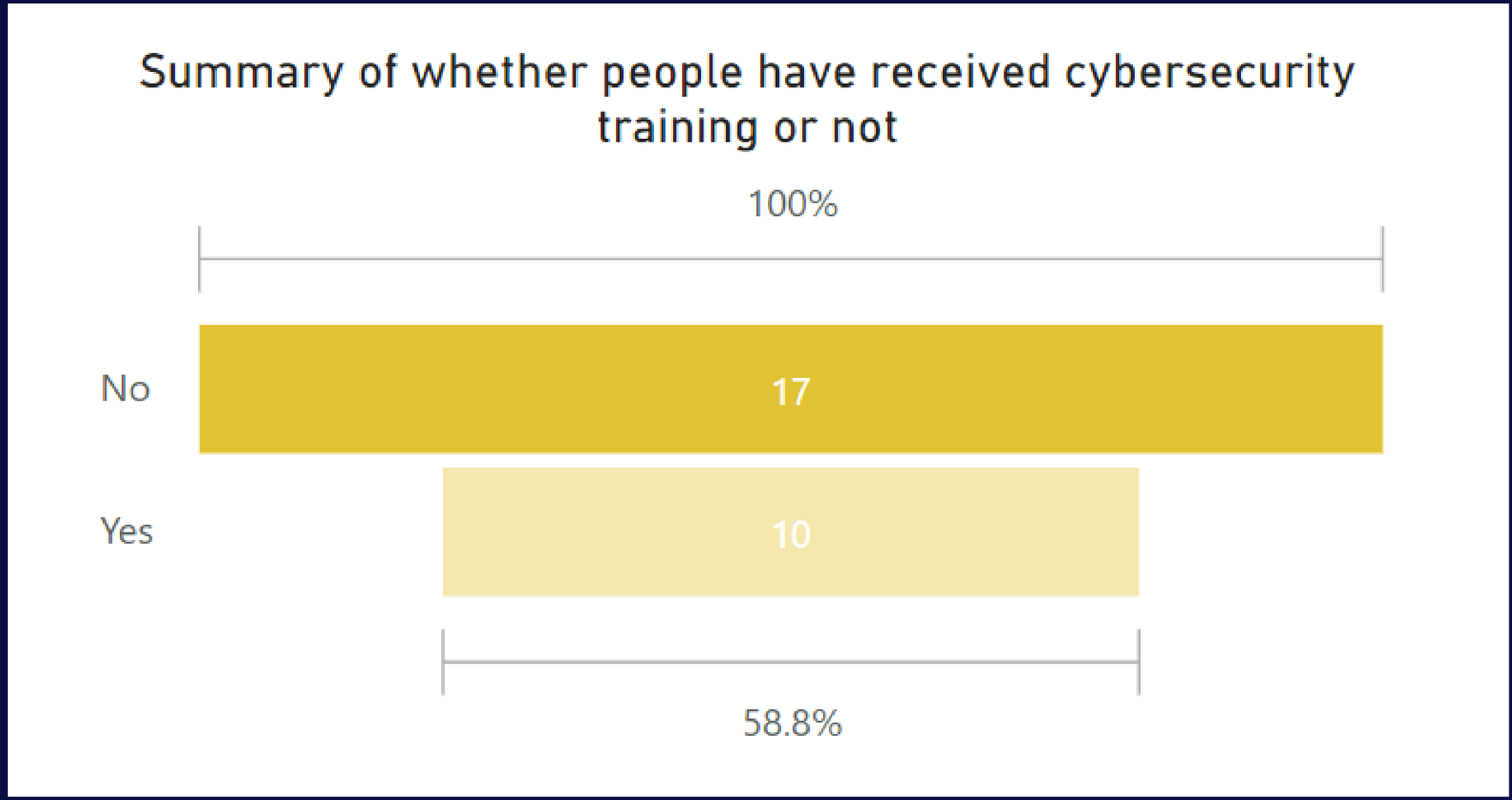


Sample’s Online Purchase Summary:

(by age groups)



Summary of whether sample has received cybersecurity training or not:



Snippet of our Data:

Age (in years)	Are the password that you use to access your bank account more complex than the password used to access your socia
20 - 35	No
36 - 59	No
Less than 20	No
20 - 35	Yes
20 - 35	Yes
36 - 59	Yes

Minimum Qualification	Please select your gender	If we create an all around approach for protecting against these threats, w
12th (HSC)	Male	Yes
Bachelors	Female	Yes

These are small snippets of our data in tabular form.

Learnings from Pilot Survey:

- As we can view from above graphs, the data is majority from 20 to 35 age group.
- We need to collect more data from age groups less than 20, 35 to 59 and senior citizens age group.
- Also, gender wise, we need a balanced sample.
- For current role, we need sample data points for retired people.
- Also, for cybersecurity training, we need to add one more question. To describe the experience.
  The purpose of this will be: If one has received training then how was it? What they learnt in that? Is it helpful in their daily lives while they work?

Feed Forward

By getting a feedback on our first form, we created a New Google Form to include Likert Scale as a measurement.

- We have added 5 relevant questions to test our hypothesis.
- Our new sample size is 39.

PFA (Google Form)

Updated Questionnaire

Q1. Are you aware about software and mobile security?

Objective: To gain insights about the awareness that user has about security.

Q2. Are your aware about Social Media Engagement & about the Victims to Social Media Attacks?

Objective: To assess the awareness and knowledge of individuals regarding social media engagement and the impact of social media attacks on victims.

Updated Questionnaire

Q.3 How often do you update your application?

Objective: To gauge the frequency of application updates among users in order to assess their engagement with and reliance on software maintenance and improvements

Q.4 Do you care about your online privacy?

Objective: Measure the respondent's level of concern for online privacy to evaluate the importance of privacy-related educational efforts and security measures.

Updated Questionnaire

Q.5 Are you aware about Cyber Security?

Objective: Assess the respondent's awareness of cybersecurity to identify the need for educational initiatives or interventions. This data will inform strategies for addressing cybersecurity concerns.

Overview of Our New Sample Data

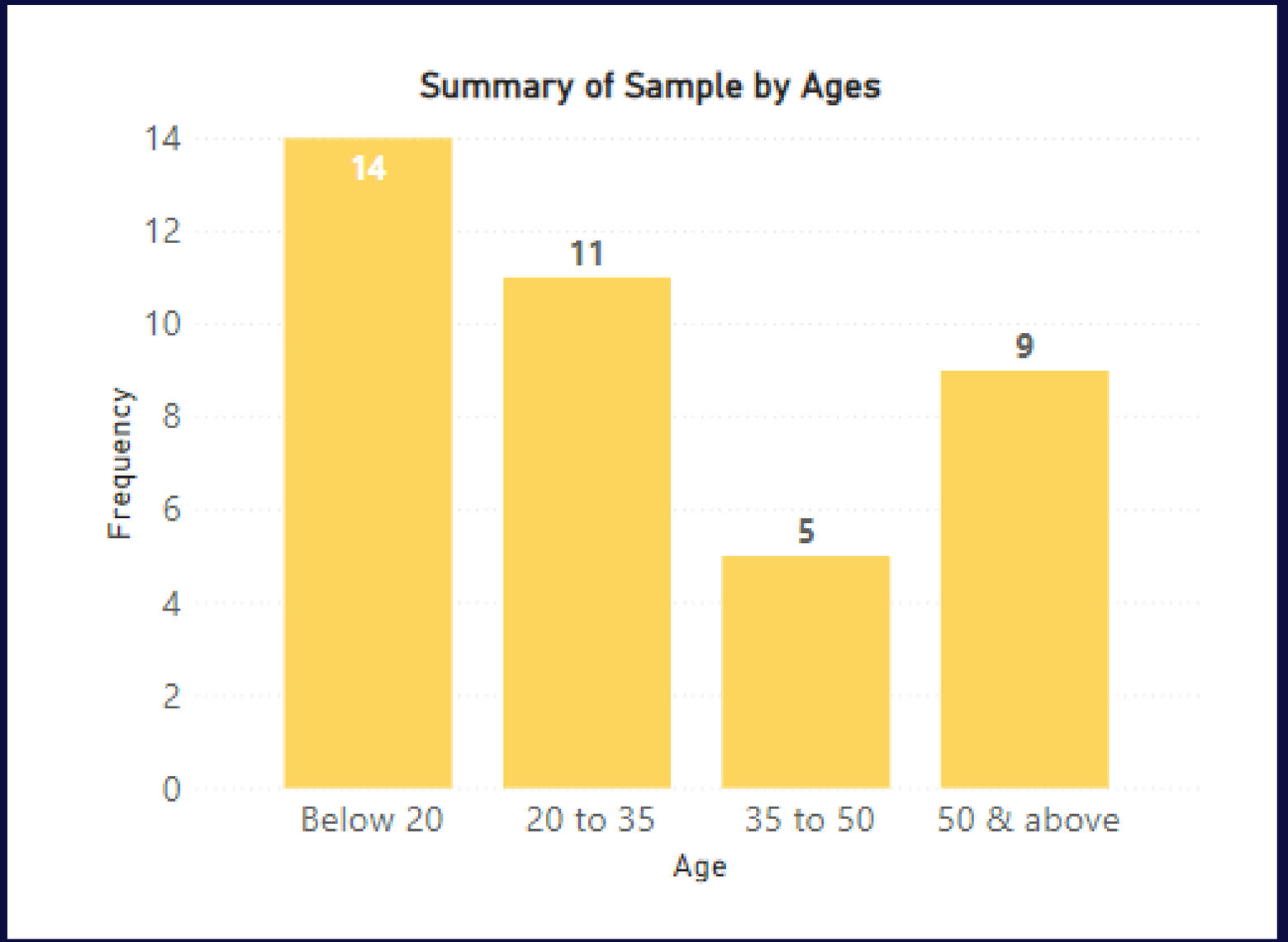
Snippet of Data

	Gender	Age	Computer Skills	Purchase Online	Software & Mobile Security	Social Media Engagement & Victim to Social Media Attacks	How often do you update your application?	Do you c
	Female	50 & above	4	1	1.5	2	2	2.
	Male	Below 20	2	2	3	3	2	
	Female	50 & above	3	2	2	1.5	1	
	Male	20 to 35	4	1	1	1	1	
	Female	20 to 35	2	2	2.5	2	2	
	Female	50 & above	3	2	3	3	3	
	Male	20 to 35	2	1	1.5	2	2.5	
	Female	20 to 35	2	2	2	2	2	
0	Male	20 to 35	2	2	2	2	2	
1	Female	20 to 35	3	2	2	2	2	
2	Female	50 & above	4	1	1	1	1	
3	Male	35 to 50	2	2	2	1.5	2.5	
4	Female	20 to 35	3	1	1.5	1.5	2	

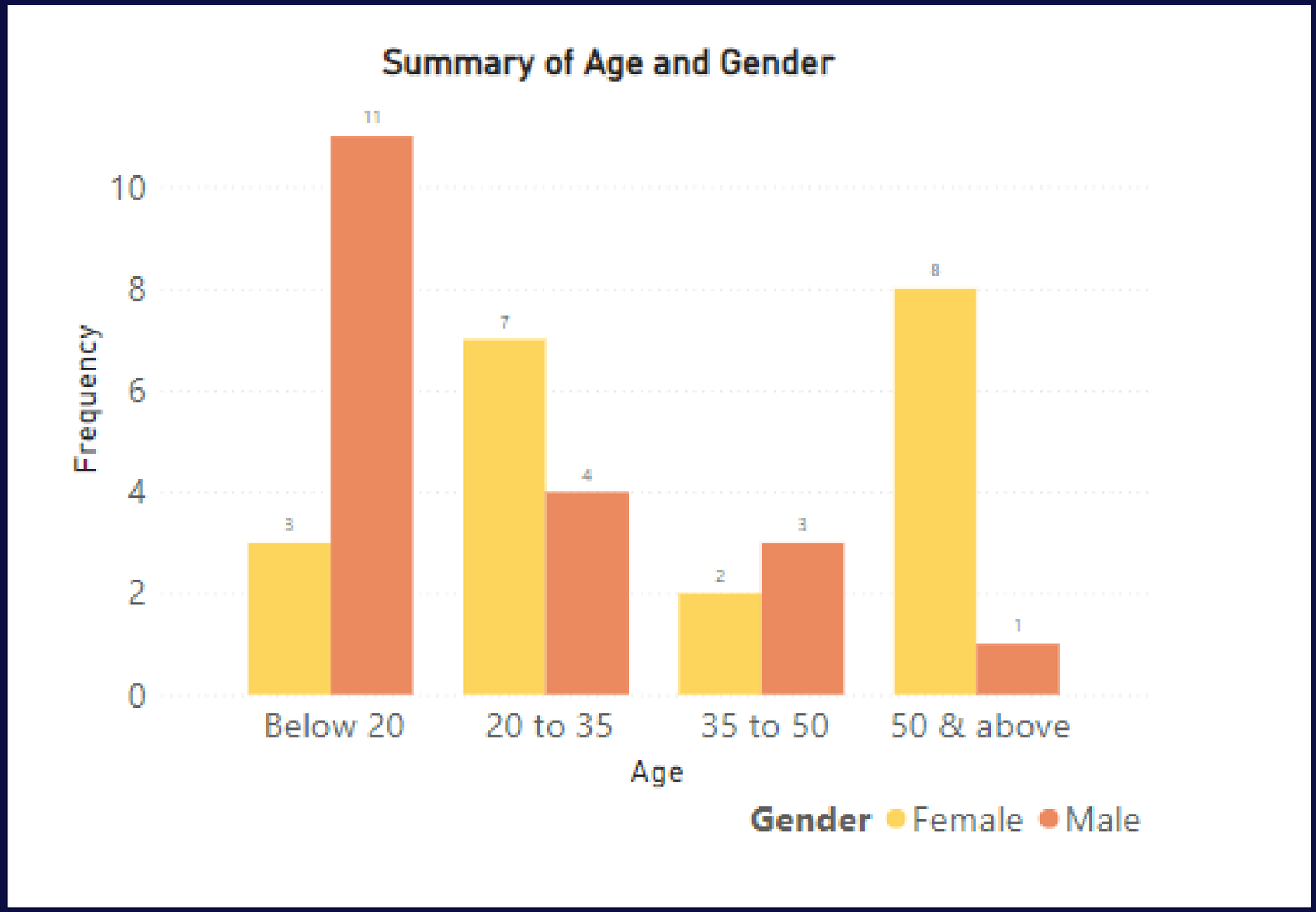
Data Summary

Sample Size: 39

Age Groups:

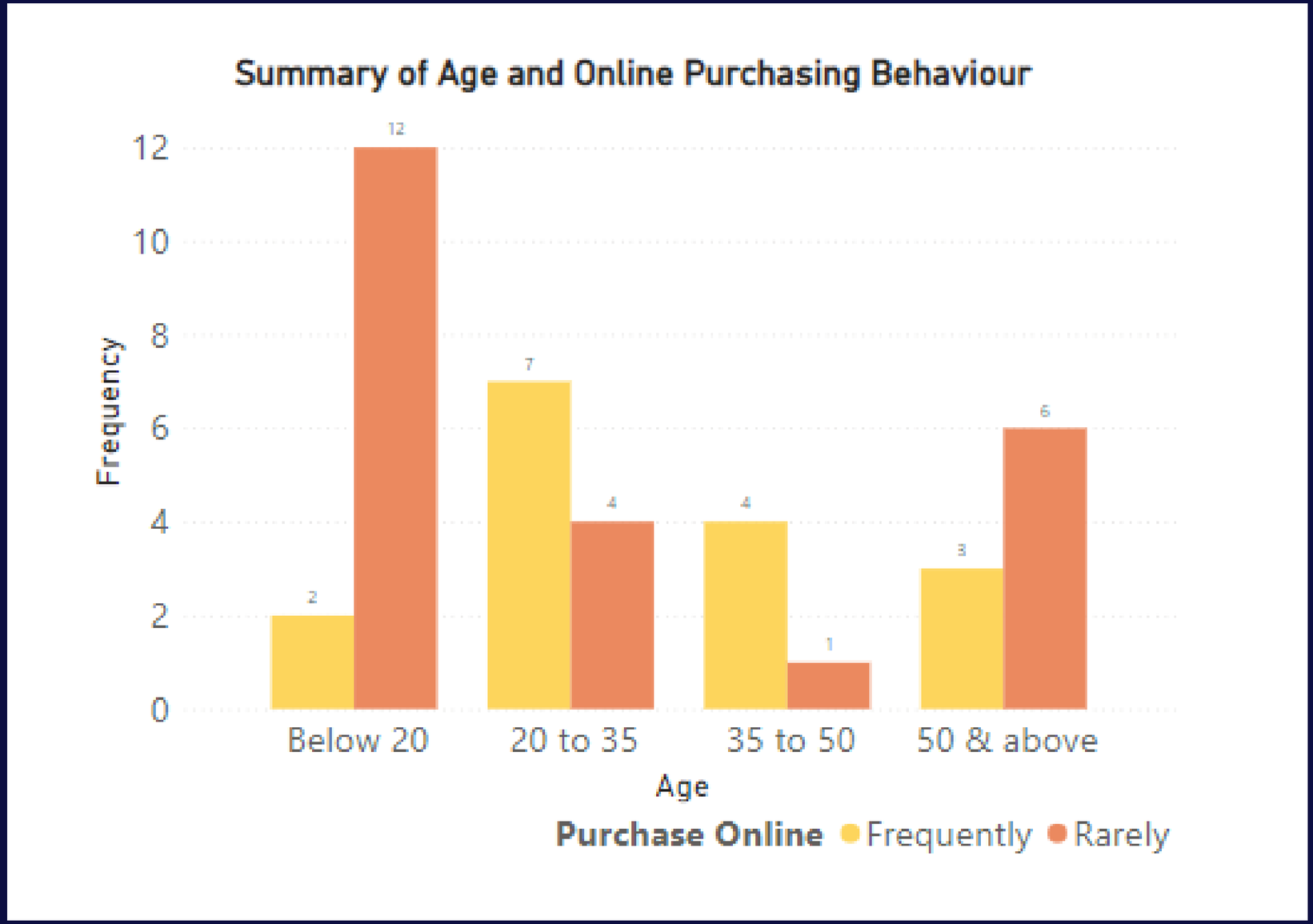


Age Groups and Gender:

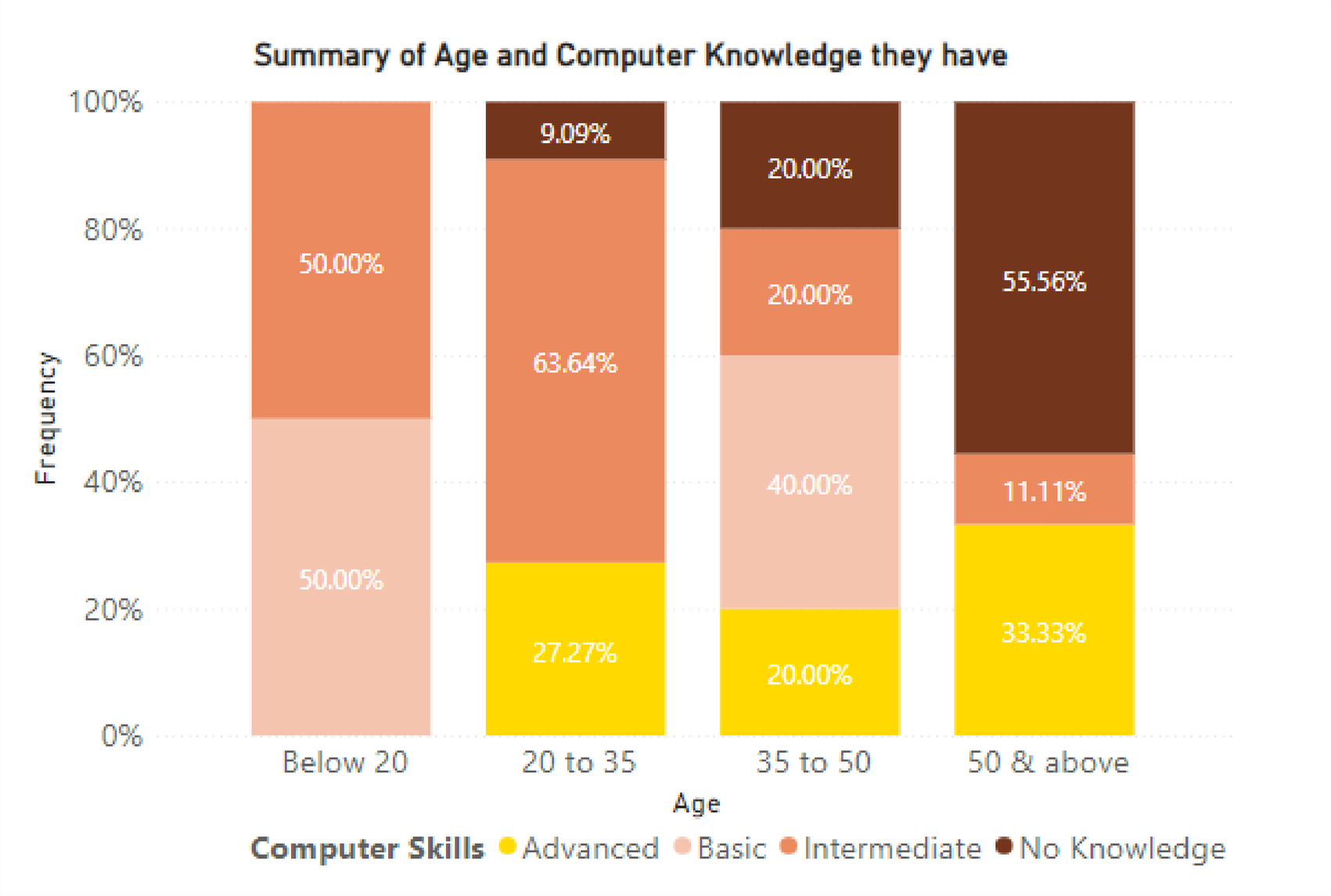


Sample’s Online Purchase Summary:

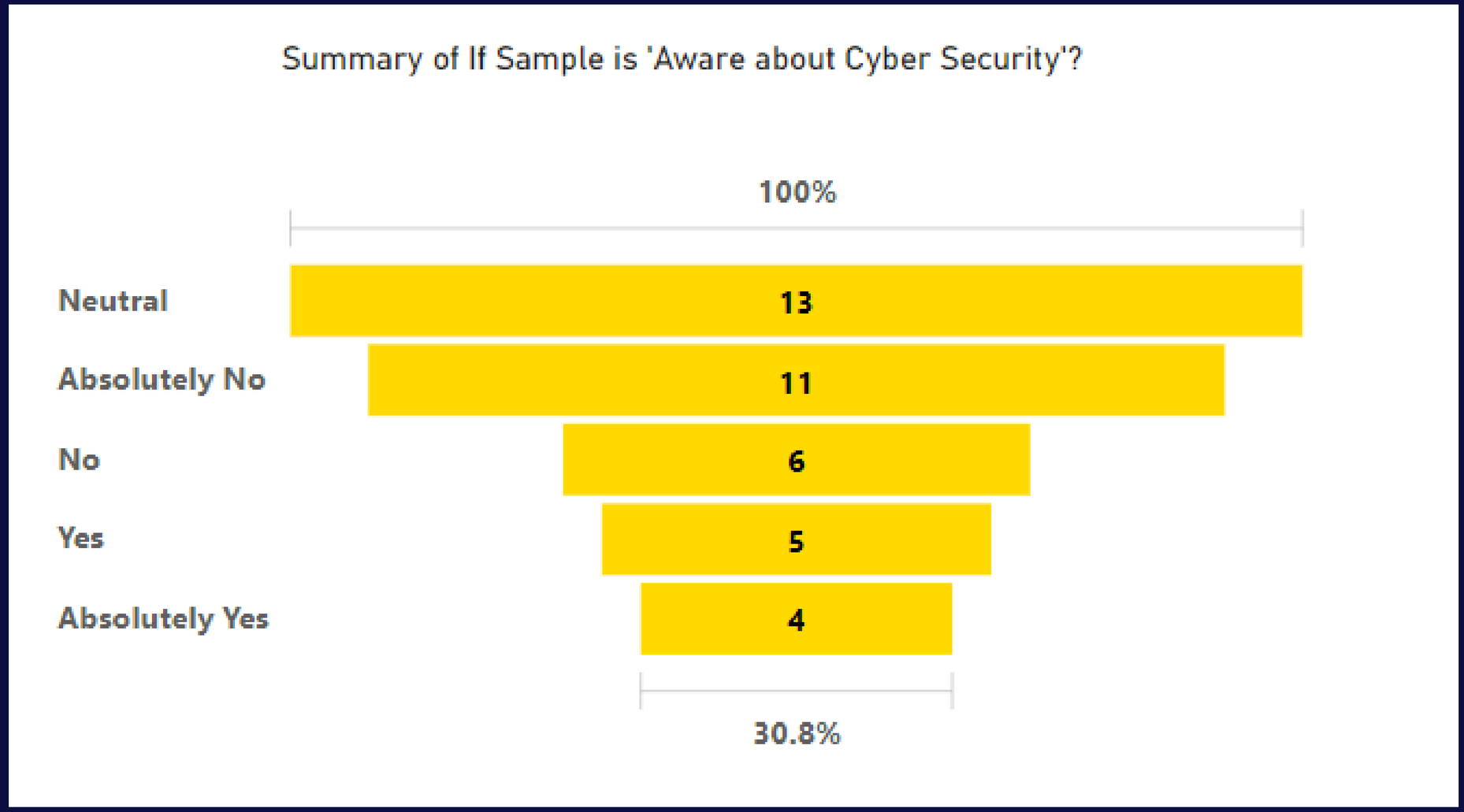
(by age groups)



Sample’s Computer Skill:



Summary of whether sample is aware about cybersecurity or not:



Statistical Analysis

Test of Reliability

The reliability test is used to determine the consistency of people’s responses across numerous items on a multiple-item measure. The Cron-bach’s alpha was utilized as a measure of consistency in the reliability test

Reliability Statistics

Cronbach's Alpha	N of Items
.759	5

The result ranges between **0.7 to 0.8**, this demonstrates that each item in the research is reliable enough.

Test of Validity

This research uses the correlation test to assess the validity of research question. The following table shows the validity test results for each item from 39 respondents.

Test of Validity

Correlations

		SoftwareMobileSecurity	SocialMediaEngagementVictimtoSocialMediaAttacks	Howoftendoyouupdateyourapplication	Doyoucareaboutyouronlineprivacy	AreyouawareaboutCyberSecurity
SoftwareMobileSecurity	Pearson Correlation	1	.585**	.377*	.640**	.457**
	Sig. (2-tailed)		.000	.018	.000	.003
	N	39	39	39	39	39
SocialMediaEngagementVictimtoSocialMediaAttacks	Pearson Correlation	.585**	1	.239	.374*	.562**
	Sig. (2-tailed)	.000		.143	.019	.000
	N	39	39	39	39	39
Howoftendoyouupdateyourapplication	Pearson Correlation	.377*	.239	1	.198	.360*
	Sig. (2-tailed)	.018	.143		.226	.024
	N	39	39	39	39	39
Doyoucareaboutyouronlineprivacy	Pearson Correlation	.640**	.374*	.198	1	.175
	Sig. (2-tailed)	.000	.019	.226		.285
	N	39	39	39	39	39
AreyouawareaboutCyberSecurity	Pearson Correlation	.457**	.562**	.360*	.175	1
	Sig. (2-tailed)	.003	.000	.024	.285	
	N	39	39	39	39	39

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

The validity coefficient (r-value) is compared to its reference criterion, which takes the value from the r table. This shows that each question is valid.

Test of Validity

Legend:

Red ovals: Denote a strong coorelation between respective variables with **99%** of confidence interval.

Green ovals: Denote a significant coorelation between respective variables with **95%** of confidence interval.

The validity coefficient (r-value) is compared to its reference criterion, which takes the value from the r table. This shows that each question is valid.

Feasibility Test of Questions

The correlation between questions item was examined using Bartlett’s test and the Kaiser–Meyer–Olkin (KMO) test. This test is used to determine the feasibility of questions that has been subjected to factor analysis.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.696
Bartlett's Test of Sphericity	Approx. Chi-Square	57.193
	df	10
	Sig.	.000

Feasibility Test of Questions

- Table shows that Bartlett’s test of sphericity has a significant value (p value) of **0.000**, which is less than 0.05. It shows that there is a relation between the questions item.
- Kaiser–Meyer–Olkin (KMO) value is **0.692** ; the KMO value is between 0.5 and 1 indicating that the questions are homogeneous.

Chi-square Test

- The chi-square test is a statistical method for evaluating the association between categorical variables in a dataset. It measures the difference between observed and expected frequencies and is often used to test independence or goodness of fit.
- Compute the Chi-Square test statistic using the formula:

$$\chi^2 = \Sigma((O - E)^2 / E),$$

where O is the observed value and E is the expected value for each category.

Hypothesis Testing

- Null Hypothesis: Software security and Mobile security has no significant effect on cybersecurity awareness
- Alternate Hypothesis: Software security and Mobile security has a significant effect on cybersecurity awareness

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	30.739[a]	16	.015
Likelihood Ratio	33.256	16	.007
Linear-by-Linear Association	7.919	1	.005
N of Valid Cases	39		

Result: The p-value is **0.015** which is less than 0.05, so we reject the Null Hypothesis and **accept the Alternate Hypothesis.**

Hypothesis Testing

- Null Hypothesis: No correlation exists between an individual's level of social media engagement / their knowledge about victims to social engineering attacks and the awareness they have.
- Alternate Hypothesis: A correlation exists between an individual's level of social media engagement / their knowledge about victim to social engineering attacks and the awareness they have.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	32.770[a]	16	.008
Likelihood Ratio	35.151	16	.004
Linear-by-Linear Association	12.003	1	.001
N of Valid Cases	39		

Result: The p-value is **0.008** which is less than 0.05, so we reject the Null Hypothesis and **accept the Alternate Hypothesis.**

Hypothesis Testing

- Null Hypothesis: There is no significant relationship between the frequency of application updates and the level of cybersecurity awareness among users.
- Alternate Hypothesis: The frequency of application updates is associated with a higher level of cybersecurity awareness, with users who update their applications more often being more security-conscious.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	26.937[a]	16	.042
Likelihood Ratio	29.865	16	.019
Linear-by-Linear Association	4.923	1	.027
N of Valid Cases	39		

Result: The p-value is **0.042** which is less than 0.05, so we reject the Null Hypothesis and **accept the Alternate Hypothesis.**

Hypothesis Testing

- Null Hypothesis: People’s awareness about cyber security and their concern about digital/online privacy are not associated.
- Alternate Hypothesis: People’s awareness about cyber security and their concern about digital/online privacy are associated.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	19.681[a]	16	.235
Likelihood Ratio	22.914	16	.116
Linear-by-Linear Association	1.169	1	.280
N of Valid Cases	39		

Result: The p-value is **0.235** which is greater than 0.05, so we **do not reject the Null Hypothesis.**

Results

For the first 3 Hypothesis, we accept the Alternate one, which implies that Cybersecurity Awareness has a significant association with following three variables:

- Software Security and Mobile Security
- Social Media Engagement and Knowledge about Victims of Social Media Attacks
- Frequency of Application Updates

This makes sense because people who have knowledge of Cybersecurity are also aware about the nitty-gritty of the Cybersecurity Domain.

Results

For the fourth Hypothesis, we do not reject the Null Hypothesis, which implies that Cybersecurity Awareness has no significant association with Individual’s Concern about their own Digital Security

This also makes sense because even though people who are not aware of the Cybersecurity Domain want to secure themselves while navigating the Digital World.

Limitations

- Limited sample size may restrict generalizability.
- Potential sample bias due to non-diverse participant selection.
- Self-reported data introduces the possibility of response bias.
- Correlations between variables are observed, but causation remains unconfirmed.
- The wording of survey questions and survey design may affect response accuracy.
- The study does not account for external factors or regional variations.
- Data collection at a single time point may not capture changes in cybersecurity awareness over time.

Future Scope

- Expand the sample size to enhance the study's representativeness.
- Investigate the impact of specific demographic factors on cybersecurity awareness.
- Consider longitudinal research to track changes in cybersecurity awareness over time.
- Conduct in-depth interviews to gain qualitative insights into participants' awareness and behaviors.
- Explore the effectiveness of cybersecurity education and awareness campaigns.
- Analyze regional or cultural variations in cybersecurity awareness and behaviors.
- Investigate the role of emerging technologies and trends in shaping cybersecurity awareness.
- Assess the potential impact of legislative changes or cybersecurity regulations on public awareness and behaviors.
- Creating a website for every age group and who are from varied background, which will give a 360 degree approach to take to safeguard oneself against Cybersecurity attacks.

Conclusions

- Software and mobile security significantly impact cybersecurity awareness.
- Social media engagement and knowledge about social engineering attacks correlate with cybersecurity awareness.
- Frequent application updates are associated with higher cybersecurity awareness.
- No significant link found between awareness of cybersecurity and concern for digital/online privacy.
- These findings reveal the multifaceted nature of cybersecurity awareness.
- Ongoing research is essential to understand evolving user attitudes and behaviors.
- Strategies are needed to enhance public awareness and online security practices.
- The digital age demands increased vigilance and education in the realm of online security.

Acknowledgement

We would like to express our sincere gratitude to **Dr. Yogesh Naik** for giving us valuable feedback and insights for our Research Project.

We’re extremely grateful for Professor’s support and guidance through this enitre journey.

Bibliography

- R. Sabillon, “)e cybersecurity awareness training model (CATRAM),” in Research Anthology on Advancements in Cybersecurity Education, pp. 501–520, IGI Global, PA, USA, 2022.

- Mcafee, “Why software updates are so important,” 2017, https://www.mcafee.com/blogs/internet-security/software-updates-important/.

- R. S. Shaw, C. C. Chen, A. L. Harris, and H. J. Huang, “)e impact of information richness on information security awareness training effectiveness,” Computers & Education, vol. 52, no. 1, pp. 92–100, 2009.

Bibliography

- A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda, “Cyber security awareness among university students: a case study,” J.Crit. Rev.vol. 7, p. 16, 2020.

- A. Moallem, “Cyber Security Awareness Among College Students,” in Proceedings of the International Conference on Applied Human Factors and Ergonomics, pp. 79–87, Orlando, Florida, July 2018.

THANK YOU