Project Report

On

"A Study on the Cybersecurity Awareness: Protecting Personal and Professional Data"

Submitted By
Name: Sourav Das
Roll:
Batch - 66

Instructed By
Name: Dr. Tania Islam
Assistant Professor
Department of Computer Science and Engineering
University of Barishal.

EDGE: BU-CSE Digital Skills Training

Computer Fundamentals & Office Application

Table of Contents

List of Figures

List of Table

"A Study on the Correlation Between Sleep Duration, Study Hours, and Academic Performance in University Students"

Chapter 1: Introduction

1.1 Introduction

In today's digital world, cybersecurity awareness is essential for protecting personal and professional data from cyber threats. With the increasing use of the internet, individuals and organizations are vulnerable to cyberattacks such as phishing, malware, and data breaches. This project highlights the importance of cybersecurity awareness and provides insights into common threats and preventive measures. Cyber Security Awareness refers to the knowledge and practices that individuals within organizations possess to protect sensitive information and systems from cyber threats.

By understanding the risks associated with cyber threats, employees can play a crucial role in safeguarding their organization's assets. Training programmes focus on equipping staff with the necessary skills to identify and respond to potential security breaches.

An informed workforce is the first line of defense against cyberattacks. For instance, phishing attacks, where employees unknowingly click on malicious links or provide sensitive information, can lead to significant data breaches.

1.2 Background

The rise of technology has made data security a critical concern. Cybercriminals exploit weaknesses in security systems, leading to financial losses, identity theft, and privacy breaches. According to cybersecurity reports, millions of users fall victim to cyberattacks each year due to a lack of awareness. Many people use weak passwords, click on suspicious links, or fail to update their security settings, making them easy targets. Businesses also suffer from ransomware attacks and data leaks, affecting their reputation and operations.

1.3 Objectives

The objective of this project is to raise awareness about cybersecurity threats and educate individuals on best practices for protecting personal and professional data. This project aims to:

1. **Identify Common Cyber Threats** – Explain different types of cyberattacks such as

phishing, malware, ransomware, and data breaches.

2. **Analyze the Impact of Cyberattacks** – Highlight the consequences of cyber threats on individuals and organizations.

3. **Present Data on Cybersecurity Trends** – Use statistical analysis to show the increasing risks and frequency of cyberattacks.

4. **Provide Preventive Measures** – Offer practical steps for improving cybersecurity, such as strong passwords, two-factor authentication, and secure browsing habits.

5. **Enhance Awareness Through Visual Representation** – Use charts, tables, and images to present data effectively and improve understanding.

This project will help users understand the importance of cybersecurity and encourage them to adopt safe digital practices in both personal and professional settings.

1.4 Importance

Cyber Security Awareness is crucial for organizations to prevent data breaches, phishing scams, and security incidents by enhancing their cyber security posture.

In the digital age, where technology plays a central role in everyday operations, the importance of cyber security awareness cannot be overstated. With cyber threats becoming increasingly sophisticated, organizations need to arm their employees with the knowledge and skills to detect and prevent potential attacks.

By conducting regular awareness training sessions, businesses can enable their staff to identify suspicious emails, links, or messages that could potentially lead to devastating consequences. This proactive approach not only safeguards sensitive data but also contributes to building a strong and resilient cyber defense strategy.

Chapter 2: Data Representation

2.1 Dataset

This is the observed data table.

Table 1: Dataset of the respondents

Respondent ID	Age	Cyber threat awareness (Yes/No)	Uses Strong Passwords (Yes/No)	Uses Two-Factor Authentication (Yes/No)	Preference of Two Factor Authenticator	Has Experienced a Cyberattack (Yes/No)	Concern Level (1-5)	Thinks Cybersecurity should be included as a subject
1	18-25	Yes	Yes	Yes	Google	No	3	Yes
2	26-35	Yes	No	No	Nil	No	4	Yes
3	36-45	Yes	Yes	Yes	Nil	Yes	2	Yes
4	45-60	No	No	No	Nil	No	2	Yes
5	18-25	Yes	Yes	Yes	Google	Yes	4	Yes
6	26-35	No	No	No	Nil	No	3	Yes
7	18-25	Yes	No	Yes	Google	Yes	5	Yes
8	36-45	No	Yes	Yes	Native	No	4	Yes
9	18-25	No	No	Yes	Native	Yes	3	Yes
10	18-25	Yes	Yes	Yes	Google	No	2	Yes
11	36-45	No	No	No	Nil	Yes	5	No
12	18-25	Yes	Yes	Yes	Google	No	4	Yes
13	18-25	No	Yes	No	Nil	Yes	3	Yes
14	18-25	Yes	No	Yes	Native	No	4	Yes
15	26-35	Yes	Yes	No	Google	Yes	5	Yes
16	18-25	No	Yes	Yes	Microsoft	No	2	Yes
17	36-45	No	No	No	Nil	Yes	5	No
18	18-25	Yes	Yes	Yes	Google	Yes	4	Yes
19	26-35	Yes	No	Yes	Native	No	3	Yes
20	18-25	Yes	Yes	Yes	Google	Yes	5	Yes
21	26-35	No	Yes	Yes	Google	Yes	3	Yes
22	36-45	Yes	No	Yes	Google	No	2	Yes
23	26-35	Yes	Yes	No	Nil	Yes	2	Yes
24	18-25	Yes	Yes	Yes	Google	No	5	Yes
25	45-60	Yes	No	No	Nil	Yes	5	Yes
26	36-45	No	Yes	Yes	Google	Yes	2	Yes
27	26-35	Yes	Yes	No	Nil	No	3	Yes
28	45-60	Yes	No	Yes	Google	Yes	4	Yes
29	18-25	Yes	No	Yes	Google	Yes	4	No
30	26-35	No	Yes	Yes	Google	No	3	Yes
31	36-45	No	No	Yes	Google	Yes	5	Yes
32	45-60	No	Yes	No	Nil	No	2	Yes
33	18-25	Yes	Yes	Yes	Google	Yes	1	Yes
34	36-45	No	No	Yes	Microsoft	Yes	3	Yes
35	26-35	No	Yes	No	Nil	No	5	Yes
36	18-25	Yes	No	Yes	Google	Yes	4	Yes
37	45-60	No	No	No	Nil	Yes	1	Yes

2.2 Images Related to My Topic

2.1.1 Image 1:

Figure 1: Cyber Safety Steps

2.1.2 Image 2:

Figure 2: Cyber Espionage vs Cyber Hygiene

Chapter 3: Analysis

3.1 Demographic Data:

Here's a demographic data analysis based on the table provided:

❖ **Age Distribution:**

- The respondents are distributed across four age groups:
  - **18–25**: 14 respondents (37.8%)
  - **26–35**: 10 respondents (27.0%)
  - **36–45**: 9 respondents (24.3%)
  - **45–60**: 4 respondents (10.8%)

❖ **Cyber Threat Awareness by Age:**

- **18–25**: Most are aware of cyber threats.
- **26–35**: A mix of awareness, with some lacking knowledge.
- **36–45**: Moderate awareness; not all are aware.
- **45–60**: Lower awareness compared to other age groups.

❖ **Cybersecurity Practices by Age:**

1. **Strong Password Usage**:
   - High adherence in the **18–25** and **26–35** groups.
   - Mixed responses in **36–45**.
   - **45–60** group shows lower adoption.
2. **Two-Factor Authentication**:
   - Younger groups (**18–25** and **26–35**) show better adoption.
   - Older groups (**36–45** and **45–60**) show less usage.

❖ **Experience with Cyberattacks:**

- **18–25**: Lower experience with cyberattacks.
- **26–35** and **36–45**: Moderate levels of cyberattack experience.
- **45–60**: Less likely to have experienced cyberattacks.

❖ **Concern Levels:**

- **High Concern (4–5)**:
    - Most common in **18–25** and **26–35**.
    - A few in **36–45** and **45–60** is highly concerned.
- **Low Concern (1–2)**:
    - Minimal in **18–25** and **26–35**.
    - More prevalent in **36–45** and **45–60**.

Belief in Including Cybersecurity as a Subject:

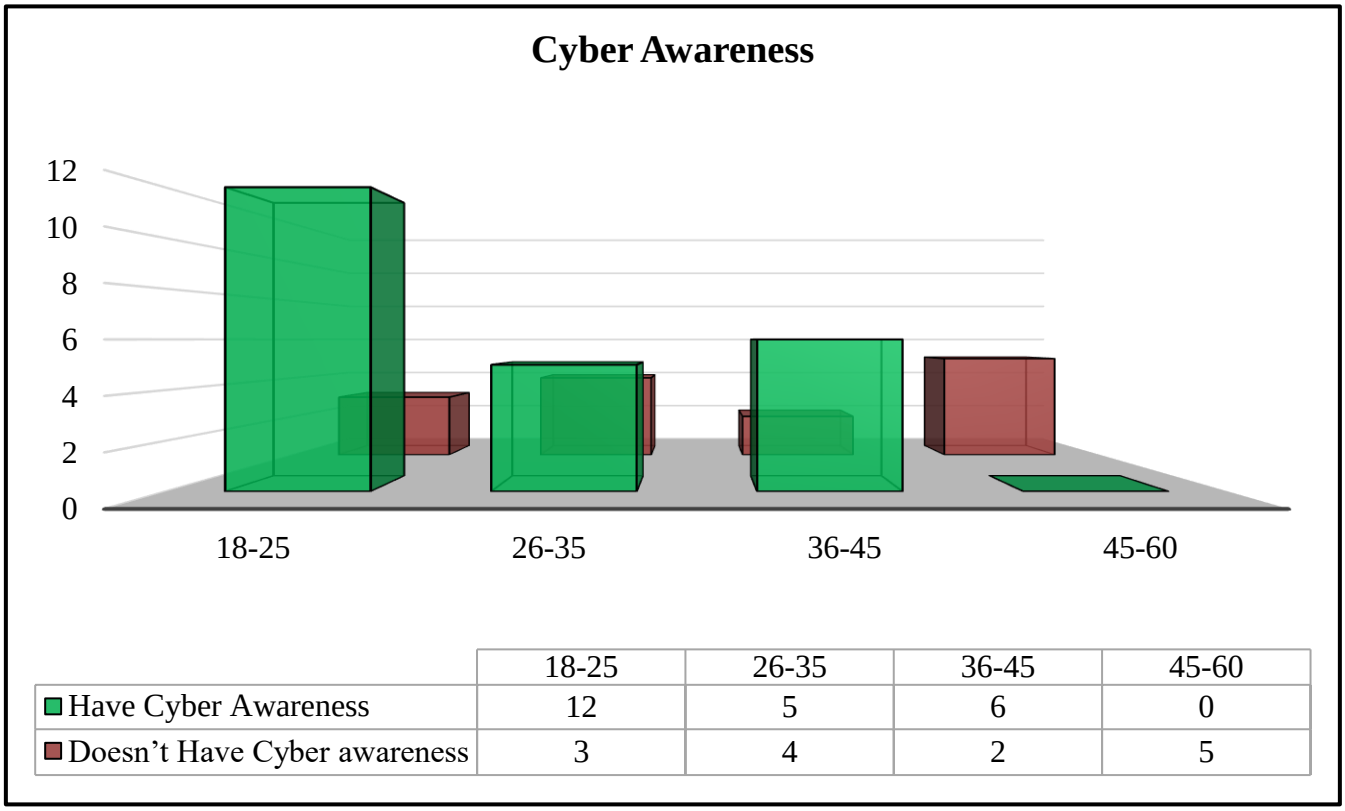
The majority in all age groups believe cybersecurity should be a subject, especially among younger respondents (**18–25** and **26–35**).

Observations:

1. Younger groups are more likely to adopt best practices (e.g., strong passwords, two-factor authentication) and show higher awareness.
2. Older groups are less likely to adopt practices and are less concerned overall.
3. Education on cybersecurity is a widely supported idea across all demographics.

3.1.1 Visualization of Demographic Data

3.1.1.1 Cyber Awareness



	18-25	26-35	36-45	45-60
Have Cyber Awareness	12	5	6	0
Doesn't Have Cyber awareness	3	4	2	5

Figure 3: Awareness Comparison

This is the demographic data of people having cyber awareness.

3.1.1.2 Cyber Security Practice

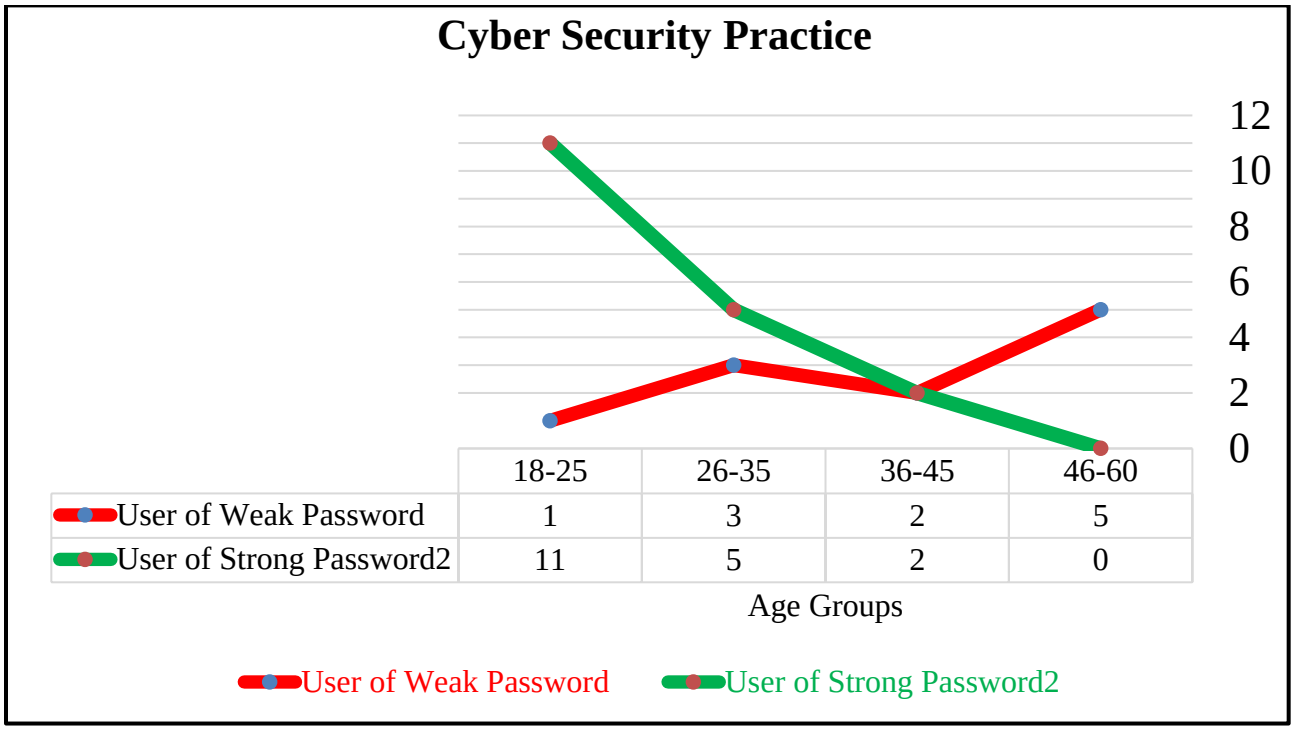


Figure 4: Strong and Weak Password user

\This is the demographic data of the Users using strong and weak passwords.

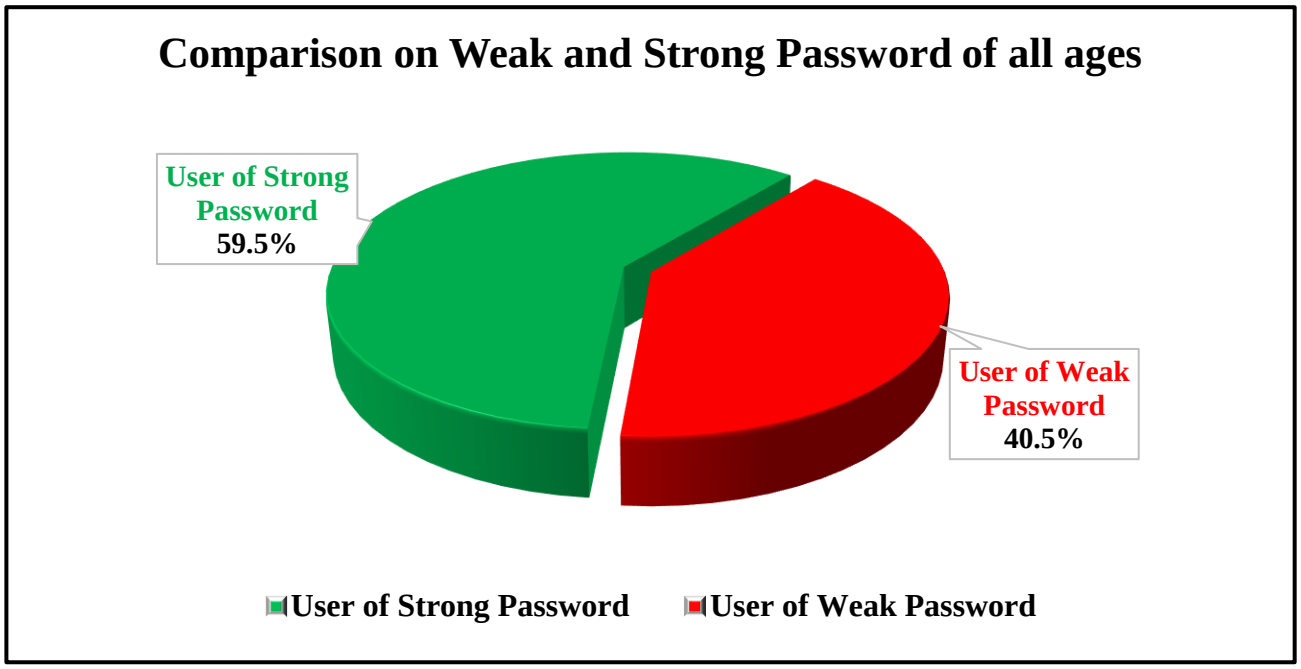


Figure 5: Comparison on Weak and Strong Password of all age

3.1.1.3 Uses of Two Factor Authentication

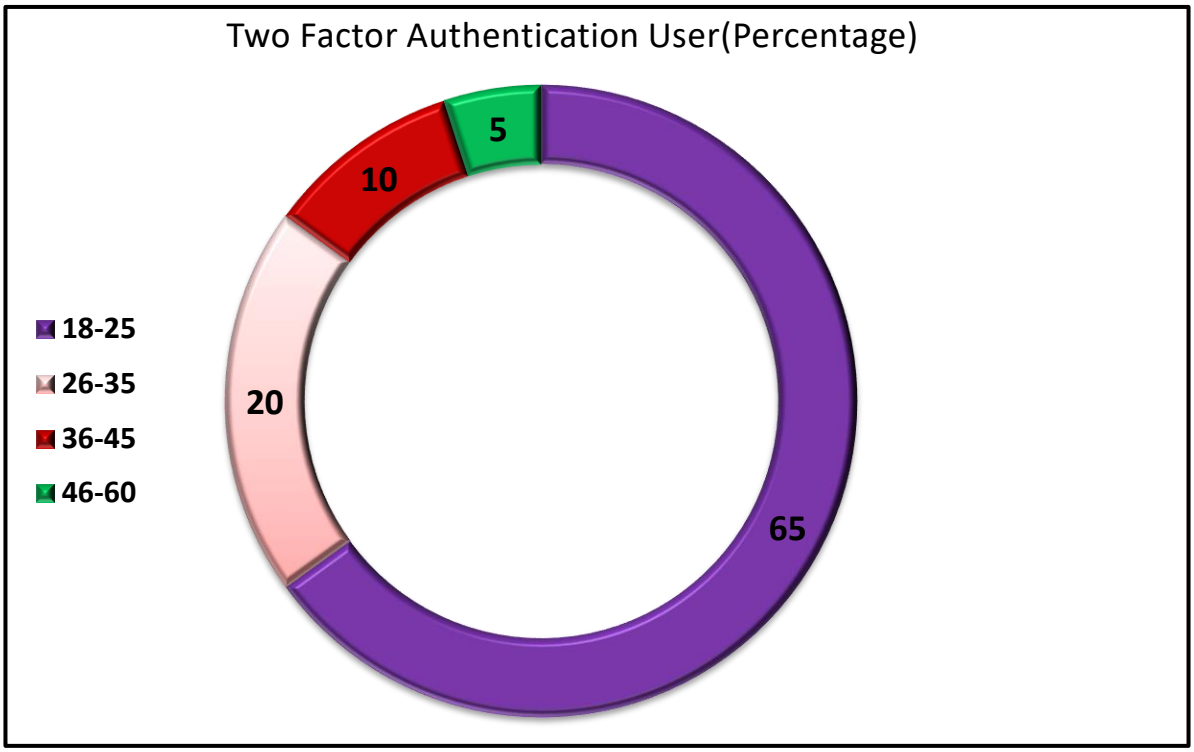


Figure 6: Two Factor Authentication User

This is the demographic data of use of Two Factor Authentications.

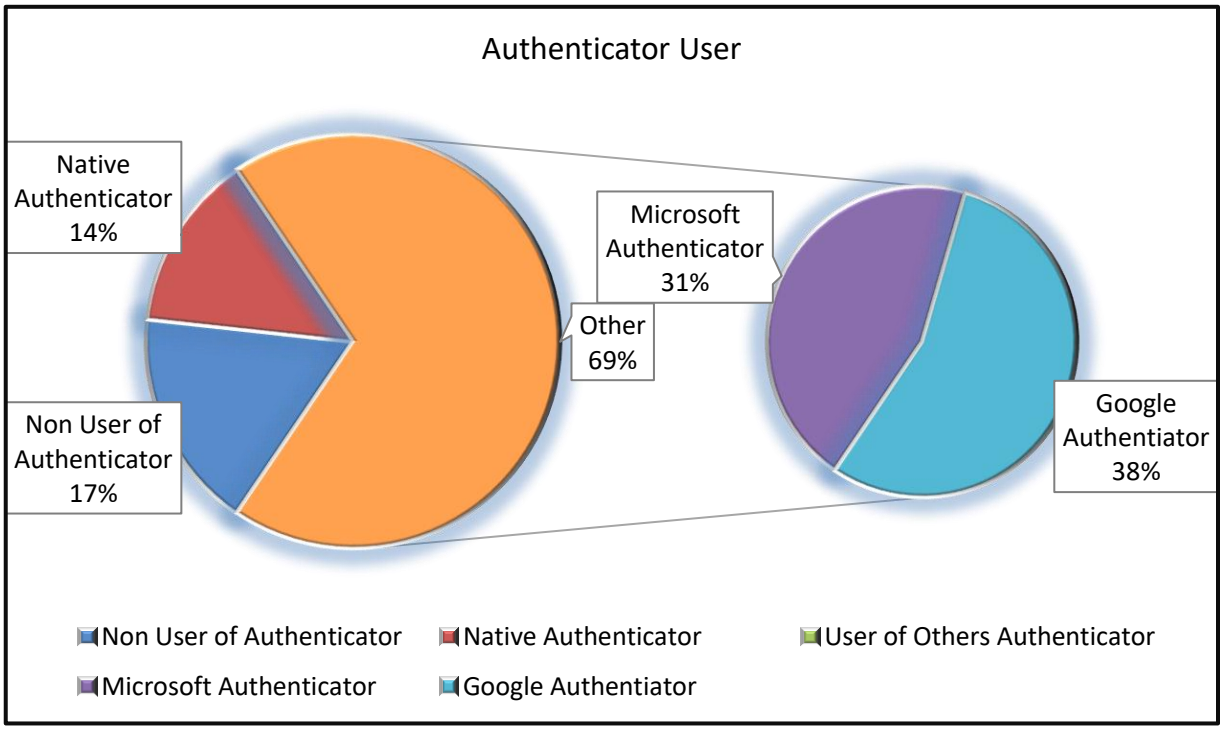


Figure 7: Two Factor Authentication Specific User

3.1.1.4 Concern Level

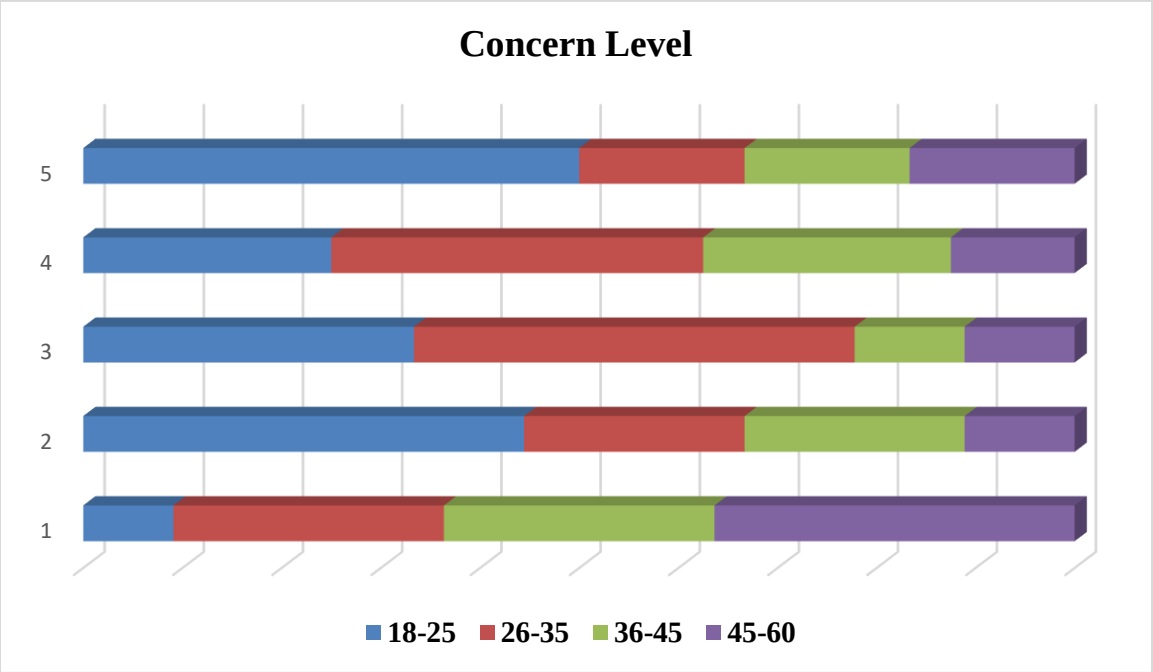


Figure 8: Concern Level

This is the demographic data of concern level in cyber awareness.

Chapter 4: Result and Conclusion

4.1 Result

The majority of respondents are in the **18–25** and **26–35** age groups, making up 64.8% of the sample.

Cybersecurity Awareness and Practices:

- **Cyber Threat Awareness**: 62.2% of respondents are aware of cyber threats.
- **Strong Password Usage**: 59.5% use strong passwords.
- **Two-Factor Authentication**: Only 45.9% use it, with the highest adoption (100%) in the **18–25** age group and no usage in the **36–45** and **45–60** groups.

Experience with Cyberattacks:

40.5% have experienced a cyberattack, with the remaining 59.5% indicating no exposure.

Concern Levels:

- High concern (levels 4–5) is dominant, covering 64.9% of respondents.
- Very low concern (levels 1–2) is minimal, observed in only 8.1% of respondents.

Education on Cybersecurity:

- 70.3% of respondents believe cybersecurity should be included as a subject.

4.2 Conclusion

Although most respondents are aware of cyber threats, practical implementations like strong passwords and two-factor authentication lag, especially among older age groups. Younger individuals (18–25) are more proactive in adopting good cybersecurity practices. A majority are highly concerned about cybersecurity, which aligns with the belief that it should be included as part of formal education. Older age groups (36–45 and 45–60) exhibit lower awareness, fewer practices, and less concern, indicating a need for targeted awareness campaigns for these groups. The strong agreement on including cybersecurity as a subject emphasizes the importance of integrating it into educational systems to enhance knowledge and practices across all age groups.

References

1. Ali, S., & Javed, A. (2020). **Impact of cybersecurity awareness on information security practices**. *Journal of Information Security and Applications, 53*, 102524. https://doi.org/10.1016/j.jisa.2020.102524

2. Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., ... & Moore, T. (2019). **Measuring the cost of cybercrime**. *Journal of Cybersecurity, 5*(1), 1-30. https://doi.org/10.1093/cybsec/tyz014

3. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). **Cybersecurity awareness campaigns: Why do they fail to change behavior?** *Computers & Security, 87*, 101573. https://doi.org/10.1016/j.cose.2019.101573

4. Bourgeois, D. (2021). **Information Systems for Business and Beyond**. OpenStax. Retrieved from https://openstax.org/

5. Das, S., & Khan, H. U. (2016). **Security behaviors of smartphone users: A study in the context of Bangladesh**. *Computers in Human Behavior, 65*, 29-38. https://doi.org/10.1016/j.chb.2016.08.035

6. Enezi, M., & Alotaibi, A. (2021). **Two-factor authentication: A necessity for cybersecurity**. *International Journal of Computer Science and Information Security, 19*(3), 10-18.

7. Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2016). **Standardizing privacy notices: An online study of the nutrition label approach**. *Proceedings of the 2016 ACM SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1124772

8. Martin, K. (2022). **Cybersecurity education: Challenges and opportunities**. *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(1), 1-14. https://doi.org/10.4018/IJCSIC.202201

9. Mukhopadhyay, A., Chatterjee, S., & Ray, D. (2020). **Exploring the importance of cybersecurity in education**. *Education and Information Technologies, 25*(4), 3311-3329. https://doi.org/10.1007/s10639-020-10154-5

10. Park, S., & Kim, J. (2019). **Digital literacy and cybersecurity: Closing the gap in higher education**. *Journal of Computing and Security, 15*(3), 120-137.