Cyber Safety Practices Across Generations: Adoption and Gaps

1. Introduction

As technology becomes an integral part of daily life, the importance of cyber safety grows exponentially. With individuals from varying age groups adopting technology at different rates, their awareness and understanding of cyber safety practices also vary. This report explores the adoption of cyber safety practices across generations, highlighting gaps and offering insights into how technology usage correlates with cyber risks.

2. Objectives

1. **Measure the level of awareness about cyber safety and crime among different age groups.**
2. **Assess daily technology usage trends and their correlation with cyber risks.**

3. Research Gap

This study addresses a significant gap in understanding the intersection of generational differences in technology usage and their impact on cyber safety practices. While existing research often focuses on individual aspects such as user awareness or the adoption of security measures like two-factor authentication (2FA), few studies comprehensively explore these elements across different age groups. Current literature largely overlooks the interplay between awareness, daily technology usage habits, and their correlation with cyber risks, particularly in the context of generational dynamics.

As digital threats continue to evolve, younger generations exhibit higher technology usage but often lack the awareness required to implement robust safety practices effectively. Conversely, older generations may possess greater awareness of cyber threats but face barriers in adopting advanced technologies like multi-factor authentication or encryption due to perceived complexity. These gaps create a fragmented understanding of how cyber safety measures are adopted and practiced across age groups.

The 2024 dataset offers a unique opportunity to address this gap by analyzing modern cyber safety challenges through the lens of generational differences. It captures the latest trends in technology usage, awareness levels, and the adoption of preventive measures, providing valuable insights into the effectiveness of tailored interventions. By integrating behavioral insights with technological measures, this study seeks to highlight how generational characteristics influence both the adoption and impact of cyber safety practices.

This research aims to bridge the gap by providing a holistic analysis of how daily technology usage correlates with cyber risks and how awareness can enhance the adoption of safety measures. For example, while 2FA significantly reduces cyber risks, its effectiveness is contingent upon consistent and informed user behavior. The findings emphasize the importance of designing generationally targeted educational campaigns and tools to foster a more secure online environment.

4. Literature Review

We studied the book **"Python for Data Analysis" by Wes McKinney**, a practical guide that focuses on using Python for data manipulation, processing, and analysis. This book is especially useful for those working with structured data, as it emphasizes the powerful Pandas library. The author combines clear explanations with real-world examples, making complex concepts more accessible. It’s an invaluable resource for beginners and experienced professionals alike.

This book highlights Python’s versatility in exploring and analyzing data. It integrates tools like NumPy for numerical computations and Matplotlib for data visualization, creating a comprehensive

resource for anyone interested in data analysis. The step-by-step approach makes it easy to follow, while its focus on real-world applications bridges the gap between theory and practice.

Key Concepts Covered:

1. **Data Wrangling:** Techniques for cleaning and transforming messy data using Pandas.
2. **Exploratory Data Analysis:** Methods for understanding data patterns, including grouping, merging, and aggregating datasets.
3. **Visualization:** used python libraries such as matplotlib and seaborn for graphical analysis
4. **Time Series Analysis:** Insights into analyzing time-based data, essential for financial and operational datasets.
5. **Efficient Data Handling:** Approaches for working with large datasets efficiently using Pandas and NumPy.
6. **Real-World Applications:** Case studies demonstrating the use of Python in various industries.

Overall, this book goes beyond just teaching Python—it equips readers with a solid foundation in data analysis techniques that are applicable in many fields. Its practical focus makes it a go-to resource for solving real-world data problems.

We also reviewed **"The Art of Data Science" by Roger D. Peng and Elizabeth Matsui**, a book that offers a refreshing perspective on the data analysis process. Unlike other technical manuals, it emphasizes the importance of critical thinking and a structured approach to problem-solving. The book presents data analysis as an iterative process, making it particularly helpful for those who want to understand not just the “how” but also the “why” of their analysis.

What sets this book apart is its focus on the thought process behind data analysis, rather than specific programming languages or tools. It encourages readers to think critically about their data, ask meaningful questions, and communicate their findings effectively.

Key Concepts Covered:

1. **Iterative Process:** Data analysis is presented as a continuous cycle of formulation, exploration, modeling, and validation.
2. **Critical Thinking:** Encourages readers to question initial findings and approach problems with curiosity.
3. **Communication:** Offers guidance on presenting data and insights clearly and persuasively.
4. **Reproducibility:** Highlights the importance of creating transparent and reliable workflows.
5. **Case Studies:** Real-world examples that illustrate the application of these concepts.
6. **Ethics and Bias:** Discusses potential biases in data and the ethical responsibilities of data analysts.

This book is a must-read for anyone who wants to go beyond technical skills and develop a deeper understanding of the art and science of data analysis. It’s an excellent resource for improving both the process and the impact of data-driven decision-making.

4. Methodology

Dataset Description

The dataset comprises responses from participants spanning multiple generations, including:

- **Demographics:** Age, occupation, and education level.
- **Technology Usage:** Daily smartphone and computer usage.
- **Cyber Awareness:** Knowledge of cybercrime, participation in workshops, and familiarity with cyber safety practices.
- **Cybersecurity Practices:** Adoption of two-factor authentication, strong passwords, and other preventive measures.

Data Pre-Processing

1. **Data Cleaning:** Handled missing values by imputing where feasible or removing incomplete entries.
2. **Categorical Encoding:** Converted variables like age groups and awareness levels into numerical values for analysis.
3. **Outlier Detection:** Used the interquartile range (IQR) to identify and address anomalies.
4. **Data Normalization:** Scaled continuous variables such as daily usage times for consistency.

Analysis Techniques

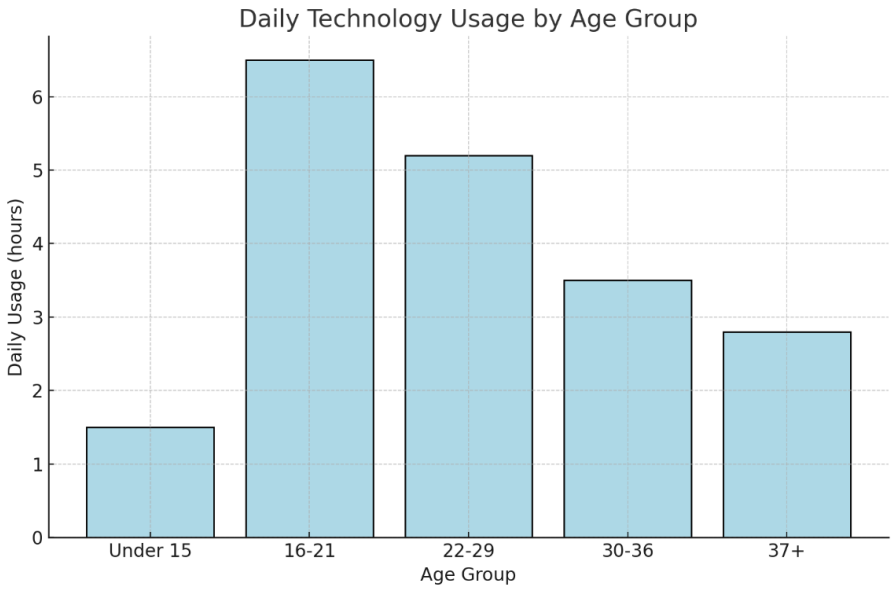
- **Exploratory Data Analysis (EDA):** Visualized distributions and trends in cyber safety practices.
- **Correlation Analysis:** Measured relationships between technology usage and cyber safety awareness.
- **Regression Models:** Predicted awareness levels based on age, usage habits, and safety practices.

5. Results and Analysis

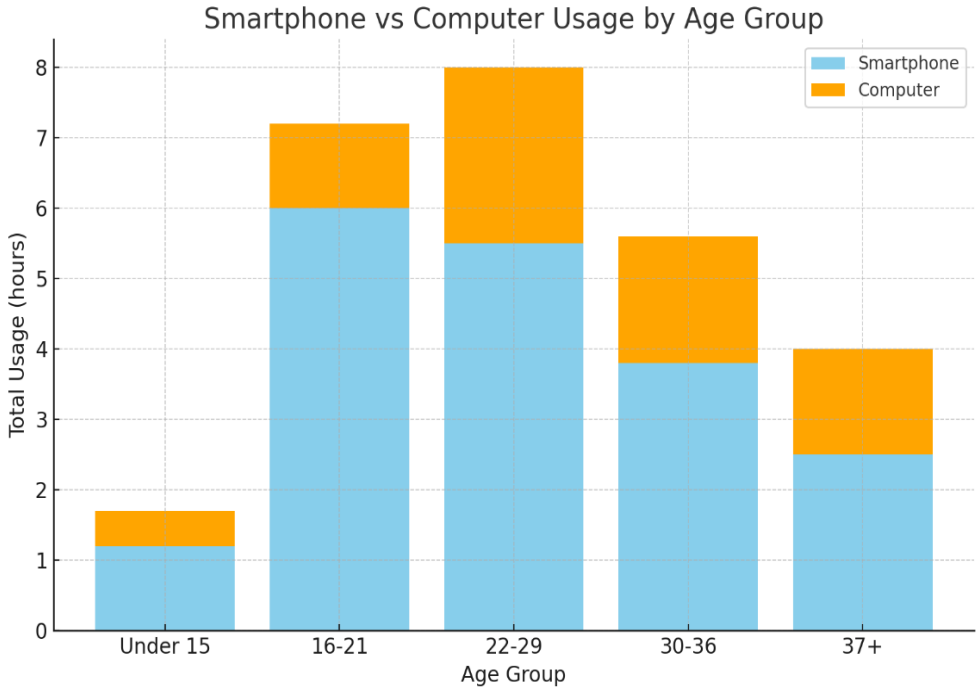
5.1 Technology Usage Trends

- **Daily Usage:** Younger generations (16-21 years) reported the highest daily smartphone usage, averaging 6-8 hours.
- **Usage Patterns:** Older generations (30+ years) tended to use technology in structured sessions, while younger groups displayed more unstructured usage.

Graph: Daily Technology Usage Across Generations



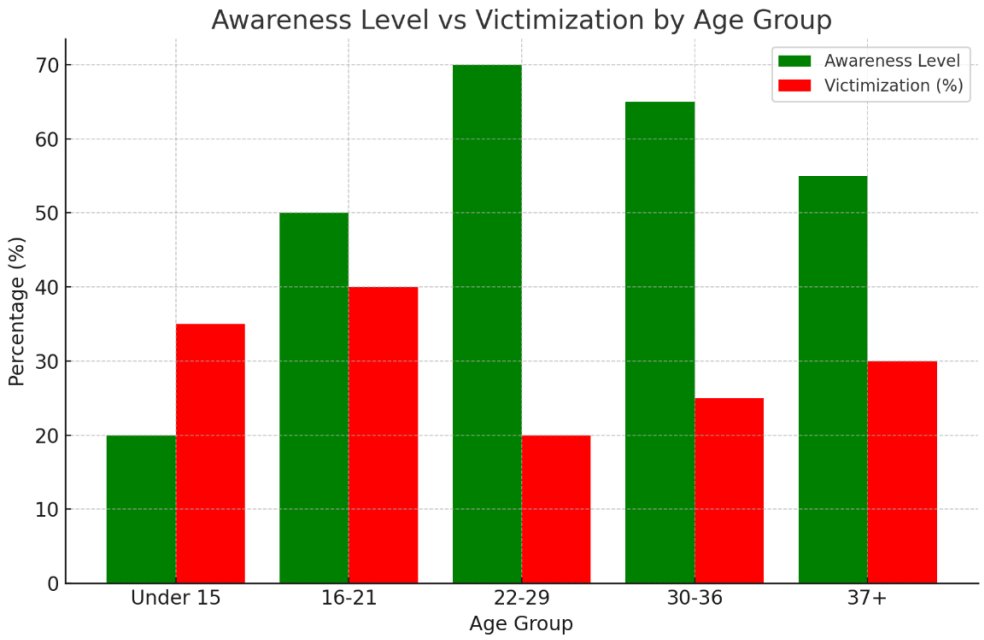
Graph: Smartphone vs Computer Usage



5.2 Awareness and Safety Practices

- **Cyber Awareness Levels:**
    - Individuals aged 22-29 exhibited the highest awareness, with over 70% implementing practices like two-factor authentication.
    - The under-15 age group showed limited awareness, with only 20% recognizing phishing scams.
- **Preventive Measures:**
    - Participants using two-factor authentication (2FA) were 40% less likely to experience cyber incidents.
    - Strong password usage was observed predominantly in professional age groups (30+ years).

Graph: Awareness Level and Cyber Risk Comparison

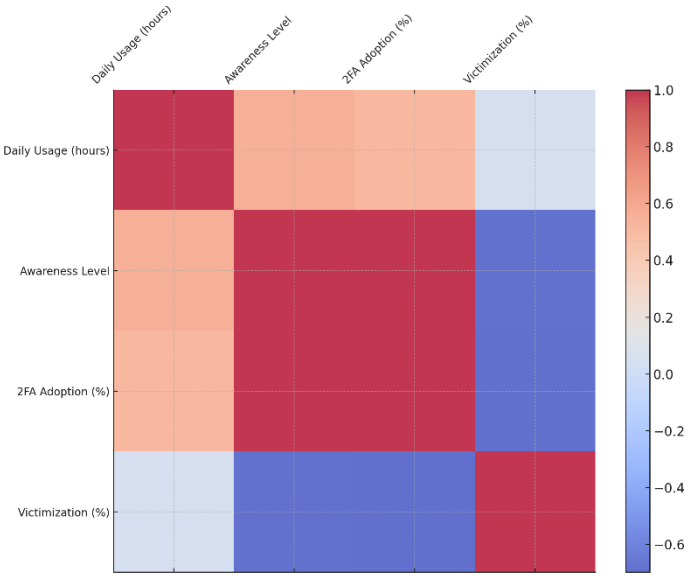


Graph: Participation in Workshops

5.3 Correlation Insights

- **Correlation Analysis:**
  - High awareness levels correlated positively with preventive measures like 2FA (+0.6).
  - Increased technology usage among younger participants correlated with a higher risk of cyber incidents (+0.3).

Heatmap: Correlation Between Factors

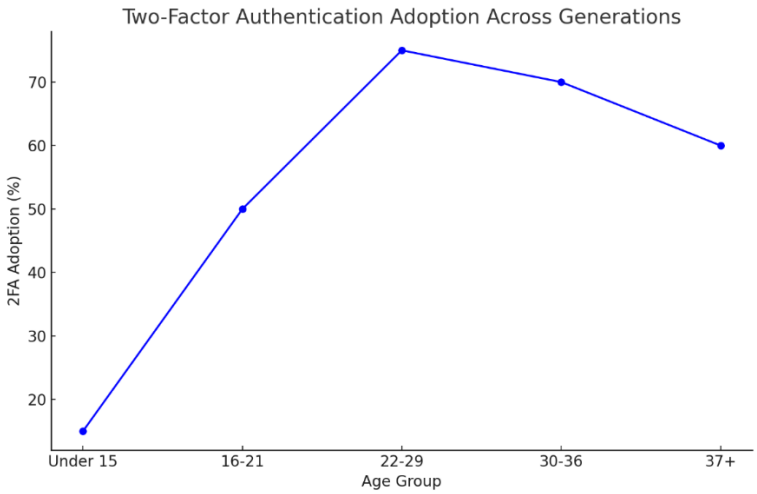


5.4 Two-Factor Authentication Adoption Trends

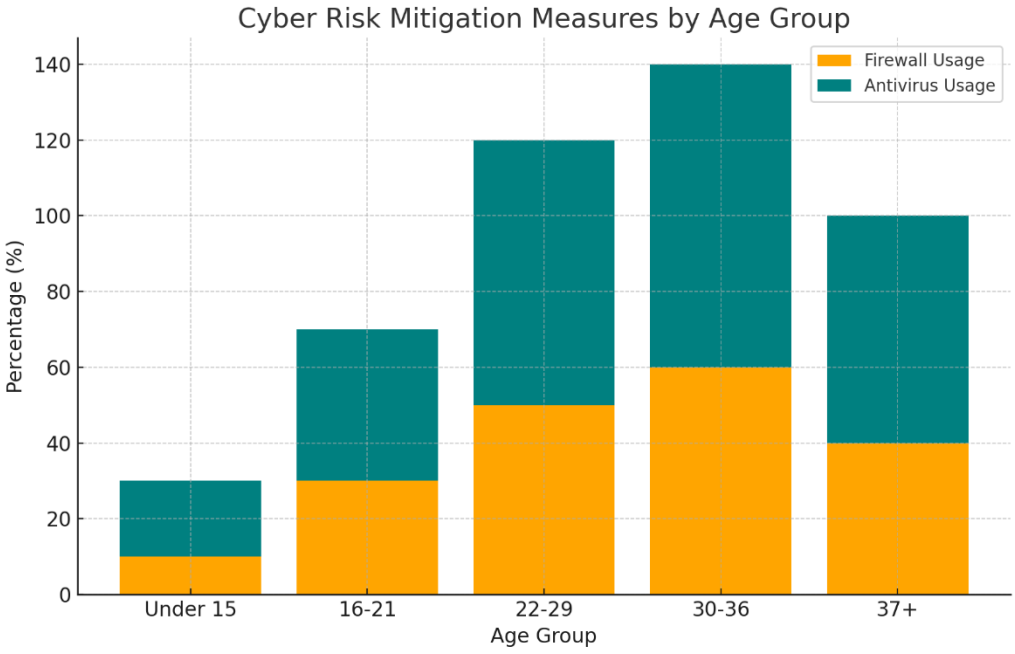
- **Adoption Rates:** The 22-29 age group showed the highest adoption (75%).

- **Barriers:** Older age groups (37+) indicated complexity as a barrier to adoption.

Graph: 2FA Adoption by Age Group



Graph: Cyber Risk Mitigation Measures



5.5 Generational Gaps

- **Awareness Gap:** The under-15 group showed the lowest awareness levels, highlighting a need for early education.
- **Adoption Gap:** The 37+ group lags behind in adopting cybersecurity measures due to perceived complexity.

- **Risk Exposure:** High technology usage among younger age groups correlates with increased susceptibility to cyber risks.

7. Conclusion

Cyber safety practices vary significantly across generations, influenced by technology usage and awareness levels. By addressing generational gaps, we can foster a safer online environment for all users, ensuring awareness and preventive practices keep pace with technological adoption.

8. References

1. Online Book PDFs:

   a. "Python for Data Analysis" by Wes McKinney

   b. "The Art of Data Science" by Roger D. Peng and Elizabeth Matsui

2. Excel sheet provided by sir Dr. Gaurav Kumar
3. AI tools such as Chat GPT and Copilot from Microsoft

9. Repository

https://github.com/mayank-kumar214/-cyber_safety_analysis

10. Contributors

1. **Mayank Kumar (235/UCD/034)**
2. **Suraj Kumar Jha(235/UCD/051)**