# Capitalism and The Illusion of Choice

Student's Name

Course

Professor's Name

Date

## Table of Contents

## Anthropomorphizing Cybersecurity: How Can Large Companies Avoid Cyberattacks With a Better Understanding of Human Behavior in Cybersecurity

Cyber in cybersecurity immediately dehumanizes the term leaving a person thinking about technology, but without the human component in it, the word loses all its meaning. Human behavior is the reason behind the need for cybersecurity, and understanding it is a very effective way to prevent cyberattacks. Knowledge of the technical aspect of network security is undeniably necessary, but the demand for know-how in behavioral analysis of human cyber action is increasing.

The proposed research aims at better understanding human behavior that translates into network security threats and susceptibility to cyber-attacks.

- What are some cyber tricks that internet users often fall victim to?
- How can companies better prepare their personnel against cyberattacks?

Existing theories suggest that most hackers seek the easiest way into a network. “Advancing education for cyber security, cyber defence and cyber warfare” shows that 91% of cyberattacks happen through personalized emails (Cruz & Simoes, 2019). This is compared to nonspecific phishing emails sent to many recipients with an opening rate of around 3%.

Even though the work of other researchers has greatly helped shape the general idea of human behavior online, there still is a large number of unknowns regarding network security. The proposed study will fill a knowledge gap and greatly assist cybersecurity specialists in better educating and preparing people for avoiding future cyberattacks.

## Literature Review

As part of preliminary research, we have identified the most cited sources in other studies, providing a great deal of information that will be the basis for this research.

P.W. Singer and Allan Friedman's work titled *Cybersecurity and Cyberwar: What everyone needs to know* (2014) provides a great baseline for the proposed study as it inquires about the foundation of cyberspace and what actions present themselves as threats. As the book was published almost ten years ago, we will compare the more modern data to identify what has changed in the past decade.

A paper “Cyber security in businesses: Challenges and recovery modes” published by Kumar and Kaur in 2022, describes the models and frameworks often used in addressing the issue of cybersecurity. The paper discusses the pros and cons of such models and is a great source for defining proper methodology while remaining ethical during the research process.

## Research Design and Research Method

The proposed research aims at identifying what cyber tricks online users fall victim to and how companies can better prepare their personnel against cyberattacks. To achieve the study's goals, we will use qualitative research methodology. Using already existing databases in behavioral sciences will be the most time-efficient way to identify patterns of human behavior online.

In addition to analyzing secondary sources such as online databases, books, the international journal of cybersecurity, and blogs, we will be using primary sources. We will be interviewing experts on social and behavioral sciences, anthropologists studying human behavior online, and cybersecurity experts, ranging from professionals working for tech think tanks to high-profile experts.

### Data Collection and Data Analysis

As mentioned previously, the groundwork for the proposed study will be archival and literature research. The sources will be selected due to their relevance to the research topic. Variables such as relevance to the study's questions, publishing period, and credibility of the authors will help us narrow down the materials. The reliability of the literature will be identified by researching how often other researchers have cited selected authors. We will also conduct interviews with cybersecurity experts and anthropologists specializing in online human behavior. They will provide more current information and allow us to add more to our current knowledge. After data collection, we will introduce rigid acceptance criteria in the analysis phase, only including the interviews that provide trustworthy, novel, and relevant data. In addition, all opposing opinions to our hypothesis will be included, ensuring the reader that the research was impartial, not suit our agenda.

### Ethical Considerations

The proposed study will follow general ethical guidelines by protecting participants' rights to privacy, autonomy, and confidentiality. Therefore, participants' consent will be obtained before recording and analyzing an interview.

### Conclusion

The proposed research aims at improving the understanding of human behavior in cyberspace and how to prepare people better to avoid cyberattacks. We will employ qualitative research methodology in the research process, conducting first-hand interviews and literature research.

As P.W. Singer and Allan Friedman write in the book 'Cybersecurity and Cyberwar: What everyone needs to know 'no issue has emerged so rapidly in importance as cybersecurity. Nevertheless, there is no issue so poorly understood as this 'cyber stuff." Great effort will be put into closing the existing knowledge gap. As a result, cybersecurity professionals will have more modern and effective evidence on how to prepare their staff against cyberattacks.

# References

Cruz, T., & Simoes, P. (2019). “Advancing education for cyber security, cyber defence and cyber warfare.” In *Proceedings of the 18th European Conference on Cyber Warfare and security: ECCWS 2019: Hosted by University of Coimbra, Portugal 4-5 july 2019* (pp. 227–341). Reading, UK; Academic Conferences and Publishing International Limited.

Kumar, T., & Kaur, S. (2022). “Cyber security in businesses: Challenges and recovery modes.” *2022 2nd International Conference on Emerging Smart Technologies and Applications (ESmarTA)*. https://doi.org/10.1109/esmarta56775.2022.9935439

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. Oxford University Press.