Sonargaon University

Department of Computer Science & Engineering

Cybersecurity Awareness

Submited To
Muydul Islam
Lecturer
Dept. of Computer Science & Engineering
Sonargaon University

Submitted By
Tofayel Ahamd Tofo
ID: CSE2202026024
Batch: 27M1

Abstract

This thesis explores the critical importance of cybersecurity awareness in the modern digital landscape. With the increasing frequency and sophistication of cyber threats, understanding and implementing proper security measures has become paramount for individuals and organizations alike. This research examines various types of cyber threats, analyzes current awareness levels, and proposes comprehensive strategies for enhancing cybersecurity education and practices.

Contents

1 Introduction **2**
1.1 Background 2
1.2 Problem Statement 3
1.3 Research Objectives 3

2 Literature Review **4**
2.1 Historical Perspective of Cybersecurity 4
2.2 Current Cybersecurity Landscape 5

3 Methodology **6**
3.1 Research Design 6
3.2 Data Collection 6

4 Cybersecurity Threats Analysis **7**
4.1 Common Threat Categories 7
4.1.1 Malware Attacks 7
4.1.2 Social Engineering 8

5 Awareness Assessment **9**
5.1 Survey Results 9
5.2 Knowledge Gaps Identified 10

6 Proposed Framework **11**
6.1 Cybersecurity Awareness Model 11
6.2 Implementation Strategy 12

7 Conclusion and Recommendations **13**
7.1 Key Findings 13
7.2 Recommendations 13

A Survey Questionnaire **15**
A.1 Demographic Information 15
A.2 Cybersecurity Knowledge Assessment 15

Chapter 1

Introduction

1.1 Background

Figure 1.1: Growth of Cyber Threats Over the Last Decade

Cybersecurity has evolved from a technical concern to a fundamental aspect of modern life. The digital transformation has brought unprecedented convenience but also significant vulnerabilities.

1.2 Problem Statement

The increasing sophistication of cyber attacks coupled with low awareness levels among users creates a dangerous environment for digital assets and personal information.

1.3 Research Objectives

- To analyze current cybersecurity threat landscape
- To assess awareness levels among different user groups
- To develop effective cybersecurity awareness strategies
- To propose implementation frameworks for organizations

Chapter 2

Literature Review

2.1 Historical Perspective of Cybersecurity

Table 2.1: Evolution of Cybersecurity Threats

Time Period	**Primary Threats**	**Main Defense Strategies**
1980s-1990s	Viruses, Basic Malware	Antivirus Software, Firewalls
2000-2010	Worms, Trojan Horses	Intrusion Detection Systems
2011-2020	Ransomware, APTs	Multi-factor Authentication, Encryption
2021-Present	AI-powered attacks, Supply chain	Zero Trust Architecture, AI Defense

2.2 Current Cybersecurity Landscape

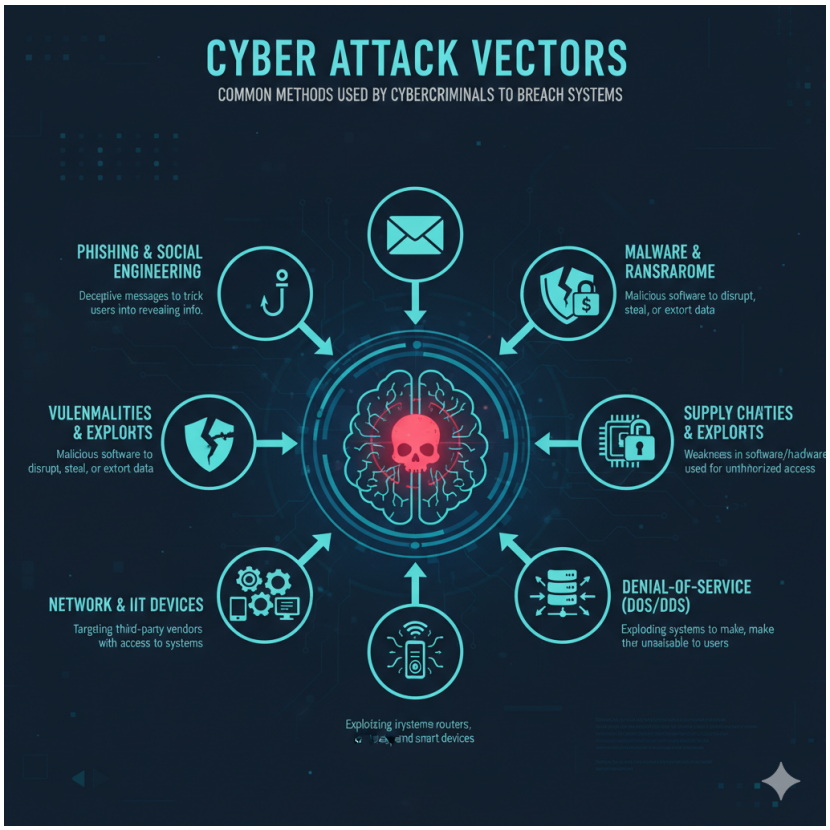

Figure 2.1: Common Cyber Attack Vectors in Modern Digital Environment

Chapter 3

Methodology

3.1 Research Design

This study employs a mixed-methods approach combining quantitative surveys and qualitative interviews.

3.2 Data Collection

Table 3.1: Data Collection Methods and Sample Sizes

Method	**Sample Size**	**Participant Group**
Online Survey	500	General Internet Users
Organizational Interviews	25	IT Professionals
Focus Groups	8 groups	Various Age Groups
Case Studies	10	Different Industries

Chapter 4

Cybersecurity Threats Analysis

4.1 Common Threat Categories

Figure 4.1: Major Cybersecurity Threat Categories and Their Impact Levels

4.1.1 Malware Attacks

Malicious software including viruses, worms, trojans, and ransomware continue to pose significant threats.

4.1.2 Social Engineering

Table 4.1: Social Engineering Attack Success Rates

Attack Type	**Success Rate**	**Average Loss**
Phishing Emails	23%	$1,500
CEO Fraud	15%	$25,000
Tech Support Scams	18%	$500
Pretexting	12%	$8,000

Chapter 5

Awareness Assessment

5.1 Survey Results

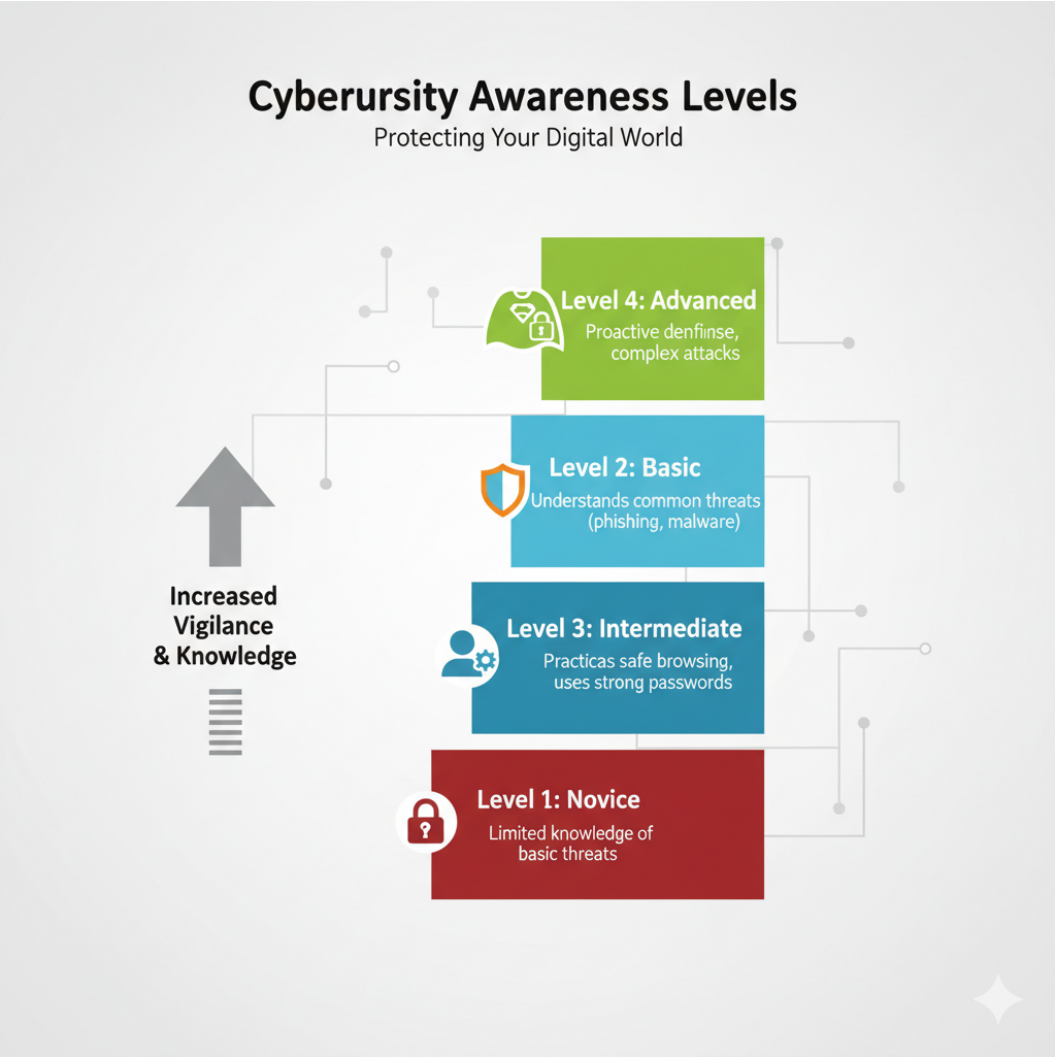

Figure 5.1: Cybersecurity Awareness Levels Across Different Age Groups

5.2 Knowledge Gaps Identified

The research identified significant knowledge gaps in:

- Password management practices
- Recognizing phishing attempts
- Understanding data privacy rights
- Secure browsing habits

Chapter 6

Proposed Framework

6.1 Cybersecurity Awareness Model

Table 6.1: Comprehensive Cybersecurity Awareness Framework

Component	**Key Elements**	**Implementation Strategy**
Education	Training modules, Workshops	Regular sessions, E-learning platforms
Policy	Security protocols, Guidelines	Documented procedures, Compliance checks
Technology	Security tools, Monitoring systems	Automated solutions, Regular updates
Culture	Behavioral change, Accountability	Leadership support, Reward systems

6.2 Implementation Strategy

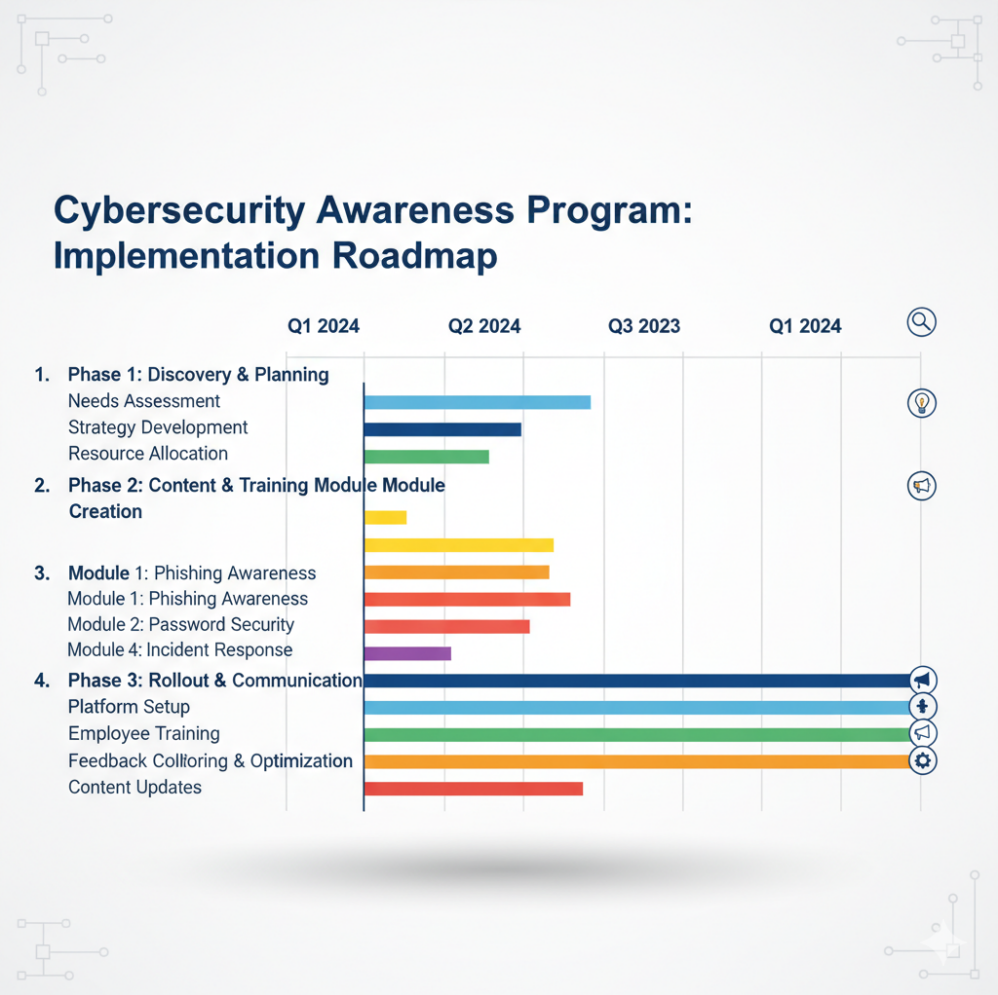

Figure 6.1: Roadmap for Implementing Cybersecurity Awareness Program

Chapter 7

Conclusion and Recommendations

7.1 Key Findings

This research demonstrates that comprehensive cybersecurity awareness programs significantly reduce vulnerability to cyber threats.

7.2 Recommendations

- Implement regular cybersecurity training programs
- Develop organization-specific security policies
- Utilize multi-layered security approaches
- Foster a culture of security awareness

Bibliography

[1] National Institute of Standards and Technology. (2023). *Cybersecurity Framework*.

[2] Verizon. (2023). *Data Breach Investigations Report*.

[3] Cybersecurity and Infrastructure Security Agency. (2023). *Cybersecurity Best Practices*.

Appendix A

Survey Questionnaire

A.1 Demographic Information

A.2 Cybersecurity Knowledge Assessment