**Title: Cybersecurity Awareness Training Program**

**Overview:**

This training program aims to equip employees with essential knowledge and skills to recognize and mitigate common cyber threats, including phishing, social engineering, and unsafe online practices.

**Duration:** 1 hour (can be adjusted based on company needs)

**Topics Covered:**

1. Introduction to Cybersecurity

2. Understanding Phishing Attacks

3. Recognizing Social Engineering Techniques

4. Best Practices for Safe Online Behavior

5. Securing Personal and Company Data

**Training Modules:**

**Module 1: Introduction to Cybersecurity**

- Definition of cybersecurity

- Importance of cybersecurity awareness

- Roles and responsibilities of employees in maintaining cybersecurity

**Module 2: Understanding Phishing Attacks**

- Definition and types of phishing attacks

- Common phishing techniques (email, SMS, voice phishing)

- Red flags to identify phishing emails

- Reporting phishing attempts

**Module 3: Recognizing Social Engineering Techniques**

- Definition and examples of social engineering

- Psychological manipulation tactics used by attackers

- Identifying warning signs of social engineering attempts

- Strategies to prevent falling victim to social engineering attacks

**Module 4: Best Practices for Safe Online Behavior**

- Creating strong passwords and using multi-factor authentication

- Safe browsing habits and avoiding malicious websites

- Being cautious with personal information sharing online

- Tips for securely managing email and social media accounts

**Module 5: Securing Personal and Company Data**

- Importance of data protection

- Handling sensitive information securely

- Encrypting data and using secure file transfer methods

- Data backup and disaster recovery procedures

**Delivery Methods:**

- Interactive presentations

- Real-life case studies and examples

- Role-playing exercises for practicing phishing and social engineering scenarios

- Q&A sessions for clarifications and additional information

**Assessment:**

- Post-training quiz to evaluate understanding and retention of key concepts

- Feedback forms for participants to provide input on the training program

**Resources:**

- Cybersecurity policy documents

- External resources such as articles, videos, and online tutorials for further learning

**Conclusion:**

By completing this cybersecurity awareness training program, employees will be better equipped to identify and respond to cyber threats, contributing to a more secure work environment for the company. Ongoing reinforcement and updates will be provided to ensure continuous improvement in cybersecurity practices.