SECURITY AWARENESS CAMPAIGN PROJECT

Presented by Tanish Rathore

INTRODUCTION

Project Objective

- This security awareness campaign is designed to educate employees and users about the importance of cybersecurity, help them recognize and respond to various cyber threats, and ensure they adopt secure practices in their everyday online activities.

Target Audience:

- The campaign is aimed at employees, students, or any group within the organization that may be at risk of cybersecurity threats.

Key Message:

- Promoting a culture of cybersecurity through education, encouraging safe practices, and reducing the risk of security incidents by fostering awareness of common cyber threats.

CAMPAIGN OVERVIEW

Duration: 4-6 weeks, with follow-up reminders.

Platform: Email, internal intranet, social media, posters, interactive quizzes, and workshops.

Theme: “Think Before You Click: Stay Secure and Safe Online”

CAMPAIGN COMPONENTS

Week 1: Phishing Awareness

• Content:
Explanation of phishing attacks and their dangers.
Interactive phishing email quiz.
Case Study of a phishing attack.

• Actions:
Encourage reporting suspicious emails.
Launch a simulated phishing test email campaign.

CAMPAIGN COMPONENTS

Week 2: Password Hygiene

• Content:

Best practices for creating strong passwords.

Benefits of using a password manager and multi-factor authentication (MFA).

Poster campaign for password security.

• Actions:

Encourage a password reset initiative using strong practices.

Host a demonstration for password manager setup and MFA configuration.

CAMPAIGN COMPONENTS

Week 3: Social Engineering

• Content:

Discuss various social engineering techniques (e.g., pretexting, baiting, tailgating).

Video series explaining social engineering tactics and prevention.

• Actions:

Organize a hands-on workshop for identifying social engineering threats.

Analyze a social engineering case study.

CAMPAIGN COMPONENTS

Week 4: Secure Browsing and Device Security

• Content:
Best practices for secure browsing, avoiding unsecured networks, and safe shopping online.
Tips for securing devices (encryption, password protection, remote wipe).

• Actions:
Promote the use of VPNs and encrypted devices.
Share reminders about updating software and device security settings.

METHODS OF DELIVERY

- **Emails/Newsletters:** Regular emails with campaign updates and resources.
- **Interactive Workshops:** Virtual or in-person sessions on key topics.
- **Posters/Flyers:** Display in high-traffic areas to reinforce messages.
- **Gamification:** Encourage participation with quizzes and challenges.
- **Videos**: Short, engaging video tutorials on cybersecurity practices.

EVALUATION AND METRICS

- **Pre-Campaign Survey:** Assess initial cybersecurity knowledge levels.
- **Post-Campaign Survey:** Measure learning outcomes and identify areas for improvement.
- **Engagement Metrics:** Track quiz completions, workshop participation, and email open rates.
- **Incident Reports:** Monitor phishing attempts and security incidents post-campaign.

FINAL REPORT

• Campaign Activities: Breakdown of each week’s focus and activities.

• Results: Analysis of campaign effectiveness using pre- and post-campaign surveys, participation rates, and metrics.

• Recommendations: Suggestions for improving future security awareness campaigns.

•Additional Resources:Cybersecurity tools, password managers, MFA apps, and links to trusted cybersecurity resources.

Thank You